UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Anja Štrukelj

Uvajanje kartičnega prometa v trgovskem podjetju

DIPLOMSKO DELO
NA UNIVERZITETNEM ŠTUDIJU

Ljubljana, 2015

UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Anja Štrukelj

Uvajanje kartičnega prometa v trgovskem podjetju

DIPLOMSKO DELO
NA UNIVERZITETNEM ŠTUDIJU

Mentor: dr. Andrej Brodnik

Ljubljana, 2015

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

IZJAVA O AVTORSTVU
diplomskega dela

Spodaj podpisana Anja Štrukelj,

z vpisno številko 63060297,

sem avtorica diplomskega dela z naslovom:

Uvajanje kartičnega prometa v trgovskem podjetju

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelala samostojno pod mentorstvom

  dr. Andreja Brodnika

- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki »Dela FRI«.

V Ljubljani, dne: Podpis avtorice:

Zahvala

Zahvaljujem se družini in prijateljem, ki so me podpirali v času študija in vem, da mi bodo stali ob strani pri vseh življenjskih preizkušnjah, ki me še čakajo.

Kazalo

Seznam uporabljenih kratic in simbolov

PCI (*ang.: Payment Card Industry*) – Industrija plačilnih kartic

PCI DSS (*ang.: Payment Card Industry Data Security Standard*) – Standard za varovanje podatkov v industriji plačilnih kartic

PCI SSC (*ang.: Payment Card Industry Security Standards Council*) – Svet za upravljanje s standardi za varovanje podatkov v industriji plačilnih kartic

PIN (*ang.: Personal Identification Number*) – Osebna identifikacijska številka

PAN (*ang.: Primary Account Number*) – Celotna številka kartice

POS (*ang.: Point of sale*) – Prodajno mesto

QSA (*ang.: Qualified Security Assessor*) – Kvalificirani ocenjevalec

SAQ (*ang.: Self-Assessment Questionnaire*) – Vprašalnik za samo-ocenitev

RKL (*ang.: Remote Key Loading*) – Oddaljeno nalaganje ključev

HSM (*ang.: Hardware Security Modul*) – Varni strojni modul

SPC (*ang.: Secure Protocol Converter*) – Varni protokolni pretvornik

DUKPT (*ang.: Derived Unique Key Per Transaction*) – Izpeljan enolični ključ transakcije

3DES (*ang.: Triple Data Encryption Algorithm*) – Šifrirni postopek, v okviru katerega se izvede DES trikrat zaporedoma. DES je blokovni algoritem za šifriranje.

ROC (*ang.: Report on Compliance*) – Poročilo o skladnosti

VLAN (*ang.: Virtual Local Area Network*) – Navidezno lokalno omrežje

SRED (*ang.: Secure Reading and Exchange of Data*) – Varno branje in izmenjava podatkov

TSP (*ang.: Tokenzation Service Provider*) – Ponudnik tokenizacije

SSL/TLS (*ang.: Secure Sockets Layer/Transport Layer Security*) – Sloj varnih vtičnic

SSH (*ang.: Secure Shell*) – Protokol za upravljanje računalnika na daljavo

TCP (*ang.: Transmission Control Protocol*) – Protokol za nadzor prenosa

MPLS (*ang.: Multiprotocol Label Switching*) – Protokol, ki v obstoječa nepovezavno usmerjena omrežja IP vpelje povezavo med končnima vozliščema

Povzetek

V diplomskem delu smo obravnavali standard PCI DSS (ang.: *Payment Card Industry Data Security Standard*), ki predstavlja enoten pristop k varovanju občutljivih kartičnih podatkov in preprečevanju zlorab v panogi plačilnih kartic. Implementacija standarda v podjetje omogoča višjo raven varnosti, ohranjanje zaupanja, zaščito pred zlorabami in posledično zaščito pred finančnimi izgubami ter izgubo ugleda.

Pri plačevanju s plačilnimi karticami so prvi člen v verigi trgovci, ki sprejemajo plačilne kartice. Takoj za njimi so na vrsti različni obdelovalci in posredovalci podatkov o plačilnih karticah. Sem spadajo procesni centri, ki so vezni členi med trgovcem in banko. Tretji člen v verigi so banke, ki imajo pogodbeno razmerje tako z imetniki plačilnih kartic kot s trgovci, ki so plačilne kartice pripravljeni sprejemati. Vse naštete organizacije morajo vpeljati standard PCI DSS v svoj sistem, če želijo poslovati s plačilnimi karticami.

V diplomski nalogi smo se osredotočili na vpeljavo standarda PCI DSS v podjetje velikega trgovca. Namen diplomske naloge je raziskati možne rešitve za vpeljavo standarda PCI DSS v podjetje velikega trgovca in ugotoviti, če je bila izbrana rešitev res optimalna izbira.

V prvem delu diplomske naloge opišemo, kaj standard PCI DSS je in katere zahteve je potrebno v podjetju velikega trgovca izpolniti, da dosežemo skladnost s standardom. Opišemo pojem PCI obseg in naštejemo razloge, zakaj je potrebno PCI obseg v podjetju čimbolj zmanjšati. V drugem delu analiziramo možne rešitve za vpeljavo standarda v podjetje. Opisan je potek implementacije izbrane rešitve v podjetje. Opišemo komponente sistema za zagotavljanje skladnosti s PCI DSS, ki so produkt lastnega razvoja. Na koncu analiziramo, če je bila izbrana rešitev res optimalna in predlagamo izboljšave ter ukrepe.

Ključne besede:

PCI DSS, vpeljava standarda v podjetje, trgovsko podjetje, kartično poslovanje, POS terminal, ponudnik varnostne rešitve

Abstract

The thesis is about PCI DSS, which stands for Payment Card Industry Data Security Standard. PCI DSS represents a unified approach to the protection of sensitive card data and to prevention of abuses in the payment card industry. Implementation of the standard in the company provides a higher level of security, it maintains confidence, protection against abuse and consequently protection against financial losses and loss of reputation.

When paying with credit cards, the first link in the chain of events is a merchant that accepts payment cards. Right behind the merchant there are different types of processors, that process payment cards information. These includes payment processing centers, which are a link between the merchant and the bank. The third link in the chain are the banks which have a contractual relationship with both the cardholder and the merchant, who is willing to accept payment cards. All of these organizations must implement standard PCI DSS in their system if they want to do business with credit cards.

In this thesis we are focused on the implementation of standard PCI DSS in the company of a large merchant. The goal of this thesis is to explore possible solutions for implementation of standard PCI DSS in the company of a large merchant and find out if the chosen solution is really the optimum choice.

In the first part we describe what standard PCI DSS is and what requirements must be met in order to achieve compliance with the standard. We describe the concept of PCI scope and name the reasons why it is necessary to minimize it. In the second part we analyze the possible solutions for the implementation of standard in the company. We described the process of implementing selected solution to the company. We describe the components of the system that are responsible for ensuring compliance with the PCI DSS, which are a product of our own development. Finally, we analyze if the selected solution was really optimal and suggest improvements and measures.

Key words:

PCI DSS, standard implementation, merchant, payment card industry, POS terminal, security solution provider

Poglavje 1

Uvod

Današnji potrošniki smo navajeni plačevanja blaga in storitev s tako imenovanim »plastičnem denarjem« oziroma plačilnimi karticami. Vstopimo v trgovino, potegnemo kartico, počakamo nekaj sekund, da se transakcija odobri in blago je naše. Toda kaj se dogaja v ozadju? So naši kartični podatki res varni pred zlorabo? Kdo vse vidi naše podatke? Ali lahko temu trgovcu sploh zaupam s svojo bančno kartico?

Prvi člen v verigi plačevanja s plačilnimi karticami so trgovci, ki sprejemajo plačilne kartice. Takoj za njimi so na vrsti različni obdelovalci in posredovalci podatkov o plačilnih karticah. Sem spadajo procesni centri, ki so vezni členi med trgovcem in banko. Tretji člen v verigi so banke, ki imajo pogodbeno razmerje tako z imetniki plačilnih kartic kot s trgovci, ki so plačilne kartice pripravljeni sprejemati.

Vodilna podjetja za izdajo plačilnih kartic so razvijala lastne programe in standarde, s katerimi so želela dvigniti raven zaščite pri procesiranju in hranjenju podatkov o plačilnih karticah. Zaradi vse večjih zlorab na področju kartičnega poslovanja so vodilni izdajatelji plačilnih kartic leta 2006 ustanovili Svet za upravljanje s standardi za varovanje podatkov v industriji plačilnih kartic (ang.: *Payment Card Industry Security Standards Council*, v nadaljevanju: PCI SSC) [5]. Svet še danes vodijo podjetja American Express, Discover Financial Services, JCB International, MasterCard in Visa Inc. Že leta 2006 so pod okriljem PCI SSC izdali prvo različico Standarda za varovanje podatkov v industriji plačilnih kartic (ang.: *Payment Card Industry Data Security Standard*, v nadaljevanju: PCI DSS) [14]. Današnja aktualna verzija je PCI DSS 3.0, ki je bila objavljena 7. novembra 2013, v veljavo pa je stopila s 1. janu-

arjem 2015. Po 1. januarju 2015 morajo biti vse organizacije, ki sprejemajo bančne kartice, skladne s standardom PCI DSS.

PCI SSC je koordinator priprave in izdajatelj varnostnih standardov na področju kartičnega poslovanja. Izdaja tri glavne sklope standardov, ki se delijo glede na različne entitete, ki nastopajo v plačilnem procesu. Ti trije standardi so:

- **PCI DSS** - Standard za varovanje podatkov v industriji plačilnih kartic
- **PCI PA DSS** - Standard za varovanje podatkov plačniških aplikacij (ang.: *Payment Application Data Security Standard*) [4]
- **PCI PTS** - Standard za varovanje transakcijskih podatkov (ang.: *PIN Transaction Security Requirements*) [13]

PCI DSS je namenjen trgovcem, ki posredno ali neposredno upravljajo s podatki o plačilnih karticah. Vsebuje nabor smernic oziroma zahtev, tako tehničnih kot operativnih, za zagotavljanje varnega ravnanja z zaupnimi, občutljivimi podatki. Namen standarda PCI DSS je zaščititi podatke o bančnih računih strank.

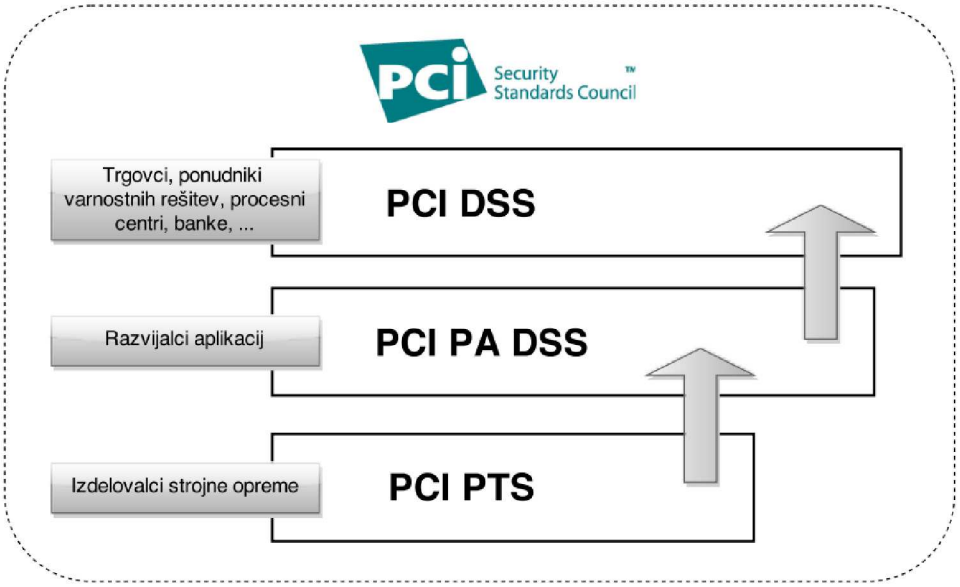
PCI PA DSS je namenjen razvijalcem varne programske opreme za obdelavo transakcij plačilnih kartic. Zahteve v tem standardu opredeljujejo predvsem varnost programske opreme skozi faze razvoja, uvedbe in vzdrževanja.

PCI PTS je namenjen razvijalcem varne strojne opreme za zajem podatkov, ki so potrebni za izvedbo transakcije s plačilno kartico. Standard natančno opredeljuje tehnično-tehnološke zahteve za varen zajem in prenos podatkov v procesu kartičnega poslovanja, kot so številka kartice PAN (ang.: *Primary Account Number*, v nadaljevanju: PAN številka), osebna identifikacijska številka PIN (ang.: *Personal Identification Number*, v nadaljevanju: PIN) ter zapis z magnetne steze ali čipa.

Slika 1.1 prikazuje hierarhijo med tremi standardi. PCI PTS predstavlja strojno plast v hierarhiji, medtem ko PCI PA DSS predstavlja programski del. PCI DSS je namenjen končnim uporabnikom, ki sprejemajo plačilne kartice.

Zahteve PCI standardov morajo upoštevati vse organizacije, ki sprejemajo, obdelujejo, hranijo ali posredujejo podatke o plačilnih karticah in njihovih imetnikih. To so:

- trgovci,



Slika 1.1: Hierarhična urejenost standardov, ki jih določa Svet PCI SSC

- procesni centri,
- finančne institucije.

1.1 Namen in cilji diplomskega dela

Cilj diplomske naloge je prikazati vpeljavo standarda PCI DSS v poslovanje velikega trgovca. Standard PCI DSS sestavljajo zahteve, ki nam povedo, kaj moramo doseči, ne povedo pa, na kakšen način naj to izvedemo. To pomeni, da je načinov za izvedbo več. Seveda želimo izbrati način, ki je dolgoročno učinkovit in predstavlja najmanj stroškov pri izvedbi.

V prvem delu bomo predstavili teoretični del diplomske naloge. Opisali in razložili bomo zahteve standarda PCI DSS, zakaj ga je potrebno vpeljati v podjetje in kakšne so posledice, če podjetje s standardom ni skladno. Prvi del naloge torej prispeva k boljšemu razumevanju področja kartičnega poslovanja in varnosti le-tega.

V drugem delu bomo preučili strokovno literaturo ter članke s predlogi možnih načinov vpeljave standarda v podjetje velikega trgovca. Najdene možne rešitve

bomo tudi ocenili in preučili njihovo primernost glede na trenutno situacijo v podjetju ter opisali prednosti in slabosti teh rešitev. V nadaljevanju bomo opisali, katera izmed rešitev je bila izbrana kot optimalna in kako smo pristopili k vpeljavi standarda PCI DSS v podjetje.

Na koncu bomo preučili, če je bila izbrana rešitev za vpeljavo standarda PCI DSS v podjetje res najboljša možna izbira. Oblikovali bom sklepe in ugotovitve ter predlagali izboljšave.

1.2 Predpostavke in omejitve

V diplomski nalogi smo se omejili na podjetje velikega trgovca ter vpeljavo standarda PCI DSS v njegovo poslovno okolje. Podjetje ni bilo skladno z nobeno od prejšnjih verzij standarda, proces vpeljave najnovejše verzije standarda 3.0 pa še ni zaključen. Trenutno je v fazi izvajanja, začel pa se je v začetku leta 2014. Zaenkrat je na 10-ih prodajnih mestih nameščeno 10 testnih POS terminalov (ang.: *Point of Sale*, v nadaljevanju: POS terminal). Cilj je nova POS arhitektura na vseh prodajnih mestih. To pomeni približno 400 prodajnih mest v Sloveniji, Hrvaški, Srbiji, Črni Gori ter Bosni in Hercegovini, torej okoli 1000 novih POS terminalov. To priča o tem, kako velik je ta projekt in kako časovno zahteven je. Ocenjujemo, da bo projekt dokončno zaključen do konca leta 2015.

Poglavje 2

Standard PCI DSS

Sledeče poglavje je ključno za boljše razumevanje kartičnega poslovanja in vpogled v področje kartičnega varovanja. Podrobneje bomo opisali pomen PCI DSS standarda in katere podatke želi standard zaščititi. Predstavili bomo, kakšne so prednosti vpeljave standarda PCI DSS v podjetje in kakšnim tveganjem smo izpostavljeni, če s standardom nismo skladni. Opisali bomo, kako začnemo uvajati standard v podjetje in kaj je najpomembnejše pri vpeljavi. Prikazali bomo, kako se izvaja testiranje skladnosti in kaj je potrebno storiti, da ohranjamo skladnost s PCI DSS.

2.1 Kaj je standard PCI DSS?

PCI DSS je globalni varnostni standard [14]. Predstavlja enoten pristop k varovanju občutljivih kartičnih podatkov in preprečevanju zlorab v panogi plačilnih kartic. Implementacija standarda omogoča višjo raven varnosti, ohranjanje zaupanja, zaščito pred zlorabami in posledično zaščito pred finančnimi izgubami ter izgubo ugleda. Namenjen je organizacijam, ki posredno ali neposredno upravljajo s podatki o plačilnih karticah. Skladnost s PCI DSS standardom se danes zahteva za vse organizacije, ki hranijo, obdelujejo in prenašajo podatke o imetnikih plačilnih kartic.

Zahteve standarda zajemajo vzpostavitev in vzdrževanje varnega omrežja, varovanje podatkov imetnikov kartic, vzdrževanje programa upravljanja ranljivosti, vzpostavitev ustreznih pristopnih kontrol, redni nadzor ter preizkušanje omrežja in vzdrževanje varnostne politike. Skladnost s standardom se zahteva

na vseh področjih poslovanja, ugotavlja pa se z lastnimi ocenjevanji ali pregledi zunanjih kvalificiranih ocenjevalcev. Vrsta ocenjevanja je v osnovi odvisna od števila letno opravljenih transakcij, če pa se v organizaciji zgodi zloraba občutljivih kartičnih podatkov, organizacija avtomatsko spada pod ocenjevanje s strani zunanjega kvalificiranega ocenjevalca.

Vpeljava standarda v poslovanje takih organizacij zagotavlja bistveno višjo raven varnosti pri ravnanju z občutljivimi kartičnimi podatki in tako omeji njihovo krajo, zlorabo ter ostale grožnje. PCI DSS standard torej velja za vse organizacije, vpletene v proces plačevanja s plačilnimi karticami. Postavlja izhodišča informacijske varnosti, ki jih morajo izpolnjevati procesni centri, banke ter prodajna mesta.

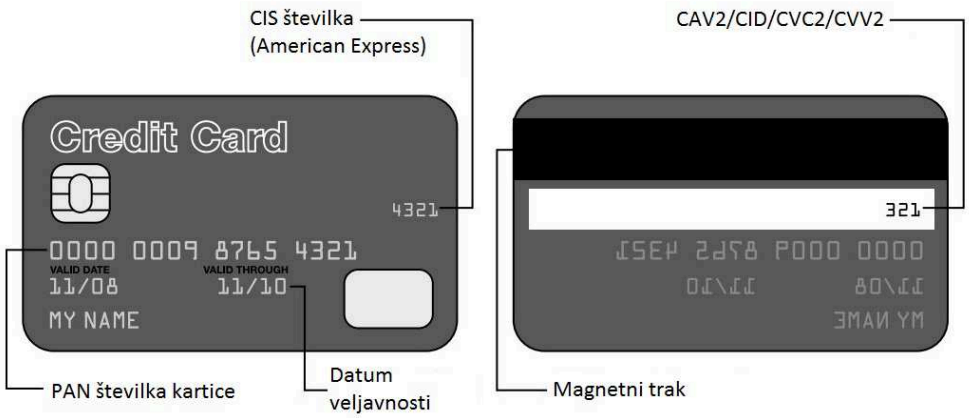
Proces vpeljave skladnosti s standardom PCI DSS ni enkratni dogodek, je proces, ki ni nikoli zaključen. Ko organizacija prejme certifikat, da je skladna s standardom PCI DSS, delo še ni končano. Štirikrat letno je potrebno narediti varnostni pregled omrežja ter spletnih aplikacij. Potrebno je izpolniti vprašalnike za samo-ocenitev oz. najeti zunanjega kvalificiranega ocenjevalca, s katerimi se učinkovito prepoznavajo in odpravljajo varnostne ranljivosti.

Glavni cilj in prva faza standarda je vpeljava vseh zahtev v poslovanje podjetja. Druga faza je ohranjanje skladnosti z več kot 220 podzahtevami, 24 ur na dan, 365 dni na leto. V primeru neskladnosti z eno podzahtevo je tveganje za vdor in zlorabo podatkov večje, nenazadnje pa obstaja tudi možnost kaznovanja podjetja s strani Sveta PCI SSC.

2.2 Podatki o imetniku kartice

Ključni faktor za vpeljavo standarda PCI DSS je prisotnost PAN številke v poslovnem okolju trgovca [14]. Če PAN številke ne hranimo, procesiramo ali posredujemo, potem zahteve standarda PCI DSS za nas ne veljajo. Poleg PAN številke procesiramo, pošiljamo ali hranimo še ime in priimek imetnika kartice, datum veljavnosti in servisno številko. Če so ti podatki prisotni v poslovnem okolju, potem morajo biti prav tako zavarovani v skladu s PCI DSS zahtevami.

Podatki o imetniku kartice so definirani s PAN številko in ostalimi elementi, ki so potrebni za obdelavo plačila. To so ime imetnika kartice, datum veljavnosti, servisna številka ter občutljivi podatki za overjanje. Občutljivi podatki za overjanje pa so podatki z magnetnega traku ali čipa, varnostna koda na kar-



Slika 2.1: Tip in lokacija podatkov na plačilni kartici.

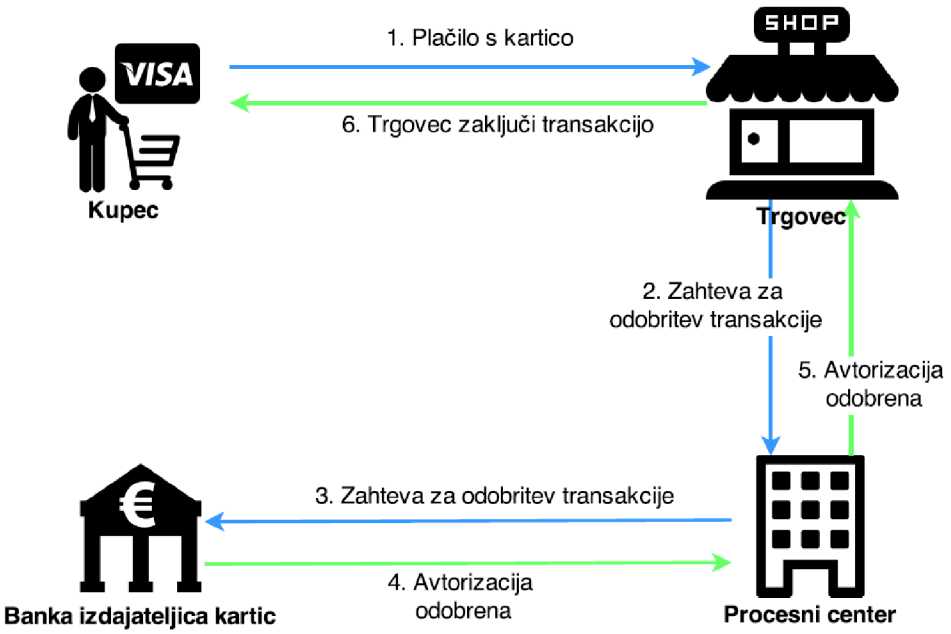
tici (CAV2/CVC2/CVV2/CID) in PIN številka (ang.: *Personal Identification Number*). Slika 2.1 prikazuje, kateri podatki se nahajajo na kartici.

Ko kupec vstavi kartico v POS terminal, se podatki s kartice zajamejo in že jih lahko začnemo procesirati. Tabela 2.1 prikazuje, katere podatke je potrebno šifrirati ter katere lahko pustimo v čisti obliki. Tabela prikazuje tudi, katere podatke lahko hranimo po izvedeni transakciji in katerih ne smemo. Občutljivih podatkov za overjanje v nobenem primeru ne smemo hraniti po izvedeni transakciji, tudi če so šifrirani.

	Podatek	Ali lahko podatek shranimo?	Ali moramo podatek podatek šifrirati?
Podatki o imetniku kartice	Številka kartice (PAN)	Da	Da
	Ime	Da	Ne
	Servisna koda	Da	Ne
	Datum veljavnosti	Da	Ne
Občutljivi podatki za avtentikacijo	Celoten magnetni zapis	Ne	Ker ni shranjen, ne šifriramo
	CAV2/CVC2/CVV2/CID	Ne	Ker ni shranjen, ne šifriramo
	PIN koda/PIN blok	Ne	Ker ni shranjen, ne šifriramo

Tabela 2.1: Shranjevanje in šifriranje podatkov skladno s standardom PCI DSS.

Pot občutljivih podatkov od zajema in preko okolja trgovca prikazuje slika 2.2. Od trgovca podatki se podatki pošljejo do procesnega centra in naprej do banke. Na sliki je prikazan primer zahteve za avtorizacijo kartične transakcije, ki se ponavadi izvede v nekaj sekundah.



Slika 2.2: Tok podatkov pri zahtevi za avtorizacijo kartične transakcije.

2.3 Struktura standarda

Standard PCI DSS sestavlja nabor tehničnih in operativnih smernic oziroma zahtev, ki sledijo primerom dobrih praks in so priporočljive za vsak sistem, kjer želimo povečati raven varnosti. Struktura standarda vsebuje šest ciljev, ki so razdeljeni na dvanajst zahtev. Vsaka od zahtev pa je še nadaljnje razdeljena na več podzahtev, vsega skupaj jih je več kot 220. Vse organizacije, ki sprejemajo plačilne kartice, so dolžne upoštevati vse zahteve standarda, razen če je to v nasprotju z lokalnimi zakoni.

Zahteve so podane v obliki tabele, v kateri je poleg vsake zahteve oz. podzahteve še postopek za testiranje le-te [14]. Tabela 2.2 prikazuje šest ciljev in dvanajst zahtev.

Za boljše razumevanje bomo podzahteve ene od zahtev tudi podrobneje opisali. Kot že omenjeno v poglavju 2.2, je odločitveni dejavnik za vpeljavo standarda PCI DSS v podjetje prisotnost PAN številke. Ena od bistvenih zahtev standarda je torej zahteva »3. Zavaruj shranjene podatke o imetniku kartice« (ang.: *3. Protect stored cardholder data*), ki se navezuje na PAN številko in ostale

Cilj	Zahteva	Pod-zahteva
Vzpostavitev in vzdrževanje varnega omrežja	1. Vzpostavi in vzdržuj konfiguracijo požarne pregrade	Vsako izmed zahtev sestavljajo še podzahteve. Vseh podzahtev skupaj je več kot 220. Pri vsaki podzahtevi so podani postopki za testiranje podzahteve.
	2. Ne uporabljaj privzetih nastavitev prodajalca za sistemska gesla in ostalih privzetih vrednosti ob namestitvi naprav	
Zaščita podatkov imetnikov kartic	3. Zavaruj shranjene podatke o imetniku kartice	
	4. Šifriraj prenos kartičnih podatkov preko odprtih, javnih omrežij	
Vzdrževanje programa za upravljanje z ranljivostmi sistema	5. Uporabljaj in redno posodabljaj protivirusno opremo	
	6. Razvij in vzdržuj varne sisteme in aplikacije	
Implementacija ukrepov za kontrolo dostopa do občutljivih kartičnih podatkov	7. Omeji dostop do podatkov samo za tiste subjekte, ki to res potrebujejo	
	8. Dodeli enolično identifikacijsko številko vsaki osebi z računalniškim dostopom	
	9. Omeji fizični dostop do podatkov o imetnikih plačilnih kartic	
Redno spremljanje in testiranje omrežij	10. Sledi in nadzoruj vse dostope do omrežnih virov in do podatkov o imetnikih plačilnih kartic	
	11. Redno testiraj varnostne sisteme in procese	
Vzdržuj varnostno politiko, ki ureja področje varovanja informacij in velja tako za zaposlene kot za zunanje sodelavce	12. Vzdržuj varnostno politiko, ki ureja področje varovanja informacij, ki velja tako za zaposlene kot za zunanje sodelavce	

Tabela 2.2: Cilji in zahteve standarda PCI DSS.

podatke o imetniku kartice. Zahtevo 3. sestavljajo naslednje podzahteve:

- **Podzahteva 3.1:** Omeji obseg in čas hrambe shranjenih občutljivih kartičnih podatkov na raven, ki še zadošča nemotenemu poslovanju. Vsako četrtletje pobriši nepotrebne shranjene podatke.
- **Podzahteva 3.2:** Ne shranjuj občutljivih podatkov za avtentikacijo (glej tabelo 2.1) po avtorizaciji, niti v primeru, da so ti podatki šifrirani.
- **Podzahteva 3.3:** Zamaskiraj PAN številko kjerkoli je prikazana. Prvih 6 številk in zadnje 4 je največ, kar smemo prikazati.
- **Podzahteva 3.4:** Kjer je PAN številka shranjena, mora biti shranjena v neberljivi obliki. PAN številka mora biti šifrirana. Tehnološke rešitve

lahko vsebujejo močne enosmerne zgoščevalne funkcije, krajšanje (ang.: *truncation*), tokenizacijo (ang.: *tokanization*) ali močno kriptografijo z ustreznih upravljanjem šifrirnih ključev.

- **Podzahteva 3.5:** Zavaruj ključe, uporabljene za šifriranje občutljivih kartičnih podatkov, pred razkritjem in zlorabo.
- **Podzahteva 3.6:** Dokumentiraj in implementiraj vse potrebne procese za upravljanje s ključi, ki se uporabljajo za šifriranje občutljivih kartičnih podatkov.

2.4 PCI obseg

Zahteve, ki jih definira standard PCI DSS, mora organizacija izpolnjevati povsod, kjer se obdelujejo, hranijo ali prenašajo občutljivi kartični podatki. Okolje, kjer se ti podatki nahajajo, se imenuje kartično okolje CDE (ang.: *Cardholder Data Environment*). Zahteve PCI DSS veljajo za vse vire, ki so v kartičnem okolju ali so z njim povezane. Kartično okolje sestavljajo ljudje, procesi in tehnologije, ki obdelujejo, hranijo ali prenašajo občutljive kartične podatke [12]. Za lažjo opredelitev virov te lahko združimo v skupine, kot so prostori in oprema, človeški viri, strojna oprema, komunikacijska oprema, programska oprema, baze podatkov ter ostali dokumenti – v fizični ali elektronski obliki. Skladnost s PCI DSS torej ni le naloga področja informatike, ampak obsega celotno poslovanje organizacije.

Za naprave in ostale vire, ki so v kartičnem okolju ali so z njim povezane, pravimo, da spadajo v PCI obseg [14]. Opredelitev PCI obsega predstavlja zahtevnejši del vpeljave standarda. Ker je izpolnjevanje zastavljenih pogojev na večjem številu naprav drago in časovno zahtevno, je prvi korak pri vzpostavljanju skladnosti s standardom PCI DSS omejevanje PCI obsega. Manj kot je naprav v PCI obsegu, manj virov je potrebnih za njihovo redno vzdrževanje. Posledično je tudi manj možnosti za vdor in zlorabo občutljivih kartičnih podatkov. Prednost manjšega PCI obsega je tudi v tem, da je ugotavljanje ter dokazovanje skladnosti s standardom PCI DSS časovno hitrejše in zato tudi cenejše.

Za zmanjšanje PCI obsega je potrebno najprej analizirati poslovne procese in opredeliti vire, ki so v kartičnem okolju ali so z njim povezani. Ugotoviti moramo, kateri podatki nastopajo v poslovnih procesih, ali so ti podatki dovoljeni

oz. sploh potrebni ter na kakšen način se bodo ugotovljeni podatki varovali. Če ugotovimo, da podatki v poslovnem procesu niso potrebni, je potrebno poslovni proces ustrezno spremeniti. Ko ugotovimo, kje vse se občutljivi kartični podatki nahajajo, lahko začnemo z zmanjševanjem PCI obsega.

Postopki za zmanjševanje PCI obsega so opisani v poglavju 3.1.

2.5 Prednosti vpeljave standarda PCI DSS

Zahteve standarda PCI DSS so tehnični in operativni napotki za trgovca. Povedo nam, katere varnostne kontrole in procese je potrebno implementirati, da bodo ustrezno zaščitili podatke o imetniku kartice. Nekatere prednosti, ki jih prinaša spoštovanje zahtev PCI DSS standarda, so:

- zaščita osebnih podatkov potrošnikov,
- povečanje zaupanja kupcev zaradi večje ravni varnosti podatkov,
- zaščita pred finančno izgubo zaradi zlorab ter stroškov sanacije,
- ohranitev zaupanje kupcev ter zaščita ugleda svojih blagovnih znamk,
- zagotovitev ustreznosti procesov, ki shranjujejo in posredujejo stranki informacije.

Zahteve standarda PCI DSS so rezultat dobrih praks, ki se jih priporoča tudi na drugih področjih poslovanja, ne samo pri kartičnem poslovanju. Velika verjetnost je, da nekatere od teh zahtev podjetje že uporablja pri svojem običajnem poslovanju (ang.: *business as usual*). Z implementacijo standarda PCI DSS lahko povečamo varnost celotnega sistema in morda pokrijemo zahteve kakšnih drugih standardov, ki se zadevajo našega poslovanja.

2.6 Tveganja pri neuvedbi standarda PCI DSS

Največje tveganje, ki se podjetju trgovca lahko zgodi v primeru neskladnosti s standardom PCI DSS, je vdor v sistem oziroma kraja kartičnih podatkov. S tem je povezano tudi veliko stroškov za raziskovanje vdora, odvetnike, poravnave, kazni ipd. Nekatere posledice vdora in kraje podatkov so:

- izguba zaupanja strank,

- zmanjšanje ugleda podjetja,
- zamenjava kadrov,
- finančne kazni zaradi neskladnosti s PCI DSS,
- povečani stroški pri ocenjevanju skladnosti, saj se v primeru vdora zahteve standarda pregledujejo še bolj striktno,
- prepoved sprejemanja bančnih kartic,
- finančne izgube zaradi zlorabe podatkov bančnih kartic,
- stroški povezani z izdelavo novih bančnih kartic,
- reševanje pritožb in s tem povezani stroški,
- stroški tožb in pravnih poravnav,
- ...

Standard je uradno izšel 7. novembra 2014, tako da so imele organizacije, ki procesirajo, hranijo ali posredujejo občutljive kartične podatke 14 mesecev časa, da zagotovijo skladnost s standardom PCI DSS. Rok za uskladitev poslovanja s standardom je bil 1. januar 2015. Ker gre pri doseganju skladnosti s standardom za obsežen projekt, je bilo nujno pravočasno začeti s pripravami. Pritisk na trgovce in procesne centre so izvajale banke, pritisk na banke pa izdajateljice kartic. Banke so pritisk lahko izvajale v obliki vse višjih provizij za transakcije, v najslabšem primeru pa bi se lahko odločile za prekinitev poslovanja s trgovcem, ki ni skladen s PCI DSS.

Odkar je standard uradno začel veljati, torej od 1. januarja 2015, banke pod pritiskom izdajateljev kartic preverjajo večje trgovce, če jim je uspelo implementirati vseh 12 zahtev iz tabele 2.2. Bankam je potrebno predložiti certifikat o skladnosti s standardom PCI DSS ali pa vsaj predstaviti ustrezna dokazila, da je standard v procesu uvajanja. V naslednjih fazah je predvideno zaračunavanje kazni za tiste trgovce, ki ne bodo skladni standardom. Načrtovane kazni se bodo vsakih nekaj mesecev progresivno povečevale, znašale pa bodo od 20.000 do 100.000 evrov mesečno. Če tudi ti ukrepi ne bi dosegli pričakovanj, se lahko kartični izdajatelji odločijo, da določenemu trgovcu, ki ne izpolnjuje zahtev, prepovejo sprejemanje kartic. Če pa se zgodi vdor v podjetje, je kazen 100.000 evrov za posamezni incident.

Problem pri katerem koli varnostnem sistemu je, da varnosti stoodstotno ne moremo zagotoviti. Vsakodnevno se namreč pojavljajo nove tehnologije in

orodja, ki ogrožajo varnost podatkov v organizacijah. Poslovodstvu tako ne moremo zagotoviti, da z uvedbo standarda PCI DSS do kraje podatkov ne bo prišlo. Lahko pa jim predstavimo zmanjšanje tveganja z ustrezno uvedbo zahtev, vzdrževanjem varnostnih kontrol in nadzorom nad procesi, ki jih upravljajo.

2.7 Testiranje in ohranjanje skladnosti

Ob vsaki izmed dvanajstih zahtev iz tabele 2.2 standard PCI DSS navaja tudi nabor testov, s katerimi si lahko pomagamo pri testiranju ustreznosti zahtev standarda. Predvideni testi so sicer zelo skopi in odgovorijo samo na vprašanje kaj testirati, redkeje pa tudi kako. Kako smo zahteve implementirali in kako smo jih testirali, mora trgovec opisati v poročilu o skladnosti ROC (ang.: *Report on Compliance*) [16].

Skladnost se ugotavlja z lastnimi ocenjevanji SAQ (ang.: *Self-Assessment Questionnaire*) ali pregledom kvalificiranega ocenjevalca varnosti QSA (ang.: *Qualified Security Assessor*). Kvalificiranih ocenjevalec varnosti je oseba, ki je certificirana s strani Sveta PCI SSC, da lahko opravlja ocenjevanja in potrjevanja skladnosti nekega podjetja s standardom PCI DSS [12]. Kdo ugotavlja skladnost je odvisno od več kriterijev. Trgovci so namreč razvrščeni v 4 stopnje in vsak trgovec je uvrščen v eno od stopenj. V tabeli 2.3 so prikazane posamezne stopnje in kriteriji za razvrstitev. Za ohranjanje skladnosti so v tabeli zapisane tudi zahteve, ki jih morajo trgovci izvajati kontinuirano, da ohranjajo skladnost s standardom PCI DSS. Največja razlika med trgovci prve stopnje in trgovci ostalih stopenj je v tem, da njihovo skladnost preverja zunanji kvalificirani ocenjevalec na samem mestu poslovanja.

Trgovsko podjetje, ki ga obravnavamo v tej nalogi, spada med trgovce 1. stopnje (ang.: *Level 1 Merchant*). V to skupino se kvalificira zato, ker ima več kot 6 milijonov kartičnih transakcij na leto. Skladnost s standardom PCI DSS mora torej preverjati zunanji kvalificirani ocenjevalec varnosti. Na vsako četrtletje je potrebno testirati tudi omrežje. Testiranje omrežja izvaja odobreno podjetje ASV (ang.: *Approved Scanning Vendor*), ki je potrjeno s stani Sveta PCI SSC. Seznam odobrenih podjetij najdemo na uradni spletni stani Sveta PCI SSC [7].

Ko kvalificirani ocenjevalec ocenjuje podjetje in izpolnjuje poročilo o skladnosti, mora pri vsaki zahtevi oz. podzahtevi podati odgovor. Del poročila o

PCI DSS Requirements and Testing Procedures	Reporting Instruction	ROC Reporting Details: Assessor's Response	Summary of Assessment Findings (check one) In Place	In Place with CCW	N/A	Not Tested	Not in Place
12.1 Establish, publish, maintain, and disseminate a security policy.							
12.1 Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).	▪ **Identify** the documented information security policy examined.	*<Report Findings Here>*					
	Describe how the information security policy was examined to verify that it is published and disseminated to:						
	▪ All relevant personnel.	*<Report Findings Here>*					
	▪ All relevant vendors and business partners.	*<Report Findings Here>*					
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.							
12.6.a Review the security awareness program to verify it provides awareness to all personnel about the importance of cardholder data security.	▪ **Identify** the documented security awareness program reviewed to verify it provides awareness to all personnel about the importance of cardholder data security.	*<Report Findings Here>*					
12.6.b Examine security awareness program procedures and documentation and perform the following:	▪ **Identify** the documented security awareness program procedures and additional documentation examined to verify that: • The security awareness program provides multiple methods of communicating awareness and educating personnel. • Personnel attend security awareness training: – Upon hire, and – At least annually • Personnel acknowledge, in writing or electronically and at least annually, that they have read and understand the information security policy.	*<Report Findings Here>*					
12.6.1 Educate personnel upon hire and at least annually. ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*							
12.6.1.a Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions).	▪ **Describe** how the security awareness program provides multiple methods of communicating awareness and educating personnel.	*<Report Findings Here>*					
12.6.1.b Verify that personnel attend security awareness training upon hire and at least annually.	**Describe how** it was observed that all personnel attend security awareness training:						
	▪ Upon hire	*<Report Findings Here>*					
	▪ At least annually	*<Report Findings Here>*					

Slika 2.3: Del poročila o skladnosti, ki ga izpolnjuje kvalificirani zunanji ocenjevalec. Na sliki je prikazan del podzahtev zahteve »12 - Vzdržuj varnostno politiko, ki ureja področje varovanja informacij, ki velja tako za zaposlene kot za zunanje sodelavce«.

skladnosti je za lažjo predstavo prikazan na sliki 2.3. Predlogo za poročilo o skladnosti najdemo na uradni strani Sveta PCI SSC [5]. Kot vidimo na sliki, je pri vsaki podzahtevi tudi navodilo za testiranje zahteve. Možnih odgovorov za oceno skladnosti je 5, pri vsaki podzahetvi pa mora ocenjevalec napisati tudi kratek opis glede na navodila pri posamezni podzahtevi. Vsaka zahteva ima lahko samo enega od naslednjih statusov:

Stopnje	Kriteriji za trgovce	Zahteve za ohranjanje skladnosti
1	Trgovci, ki procesirajo več kot 6 milijonov transakcij na leto ali so imeli vdor v podjetje, kjer so bili ogroženi kartični podatki	- Letno poročilo o skladnosti, ki ga izvede kvalificirani ocenjevalec - Testiranje omrežja vsako četrtletje, ki ga izvede odobreno podjetje ASV
2	Trgovci, ki procesirajo od enega milijona do 6 milijonov transakcij na leto	- Letno lastno ocenjevanje SAQ - Testiranje omrežja vsako četrtletje, ki ga izvede odobreno podjetje ASV
3	Trgovci, ki procesirajo od 20000 do enega milijona transakcij na leto	- Letno lastno ocenjevanje SAQ - Testiranje omrežja vsako četrtletje, ki ga izvede odobreno podjetje ASV
4	Ostali trgovci, ki sprejemajo bančne kartice in ne spdajo v stopnje 1, 2 ali 3	- Letno lastno ocenjevanje SAQ - Testiranje omrežja vsako četrtletje, ki ga izvede odobreno podjetje ASV

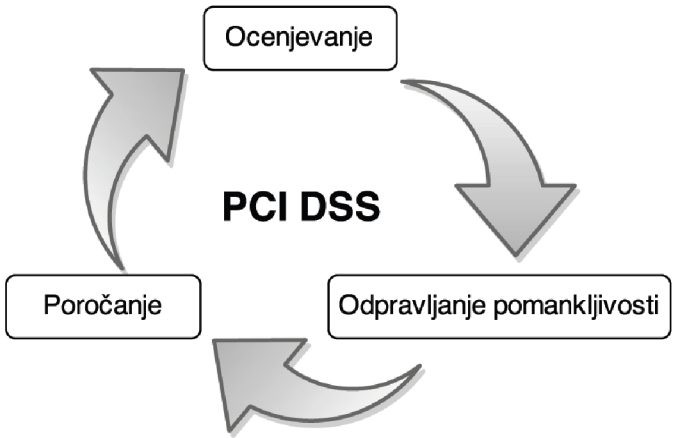
Tabela 2.3: Stopnje trgovcev, kriteriji za razvrstitev in zahteve za ohranjanje skladnosti.

- **Zahteva je na mestu** (ang.: *In place*) - zahteva dobi status »Na mestu«, če imajo podzahteve statuse, da so »Na mestu« ali pa status »Ne pride v poštev« ne pridejo v poštev za ocenjevanje skladnosti.
- **Zahteva je na mestu s kompenzacijo** (ang.: *In Place with CCW (Compensating Control Worksheet)*) - zahteva dobi ta status, če ni bila implementirana tako, kot piše v zahtevi, temveč s pomočjo neke druge rešitve. Opis kompenzacije mora biti priložen poročilu o skladnosti.
- **Zahteva ne pride v poštev** (ang.: *Not Applicable*) - če neka zahteva ne pride v poštev za okolje, ki je ocenjevano, zahteva dobi ta status. Nekatere zahteve vedno pridejo v poštev, na primer zahteva »3.2 - Ne shranjuj občutljivih podatkov za avtentikacijo (glej tabelo 2.1) po avtorizaciji, niti v primeru, da so ti podatki šifrirani«. Kljub temu, da ima zahteva status, da ne pride v poštev, je še vedno potrebno v poročilo napisati, zakaj je temu tako.
- **Zahteva ni testirana** (ang.: *Not Tested*) - v primeru, če neka zahteva ni bila testirana.
- **Zahteva ni na mestu** (ang.: *Not in Place*) - če katerakoli od podzahtev ni v skladu z navodili zahteve, potem zahteva dobi status »Ni na mestu«.

Proces ohranjanja skladnosti ni enkratni dogodek temveč kontinuiran proces. Sestavljen je iz korakov, ki jih prikazuje slika 2.4. Vsakoletno je potrebno

oceniti varnostne pomanjkljivosti okolja, kjer se kartični podatki nahajajo. Pomanjkljivosti je potrebno odpraviti in vzpostaviti varne poslovne procese. Podrobnosti ocenjevanja pomanjkljivosti in odpravljanja le-teh je potrebno dokumentirati v letnem poročilu o skladnosti in jih predati bankam. Vrstni red same vpeljave standarda v podjetje sestavljajo naslednji koraki:

1. Trgovec ugotovi, katere komponente sistema so v PCI obsegu.
2. Kvalificirani ocenjevalec varnosti izbere reprezentativno podmnožico naprav iz PCI obsega in preveri skladnost z zahtevami PCI DSS.
3. Če kvalificirani ocenjevalec varnosti ugotovi, da se nekaterih zahtev ne da popolno izpeljati, poišče načine, kako kljub temu zagotoviti skladnost s PCI DSS.
4. Trgovec odda poročilo o skladnosti ROC.
5. Če banka zahteva, mora trgovec poročilo dopolniti oz. dopisati razlago pri posameznih zahtevah.



Slika 2.4: Ohranjanje skladnosti s PCI DSS je kontinuiran proces.

Poglavje 3

Vpeljava standarda v podjetje

Zahteve PCI standardov morajo upoštevati vse organizacije, ki sprejemajo ali obdelujejo podatke plačilnih kartic. To so procesni centri, finančne institucije ter trgovci. Poudarek v tej diplomski nalogi je na kartičnem poslovanju velikega trgovca. Kaj sploh definira trgovca po PCI DSS standardu? Trgovec je poslovni subjekt, ki sprejema bančne kartice vseh izdajateljev kartic, ki skupaj tvorijo Svet PCI SSC [12]. To so kartice naslednjih izdajateljev: American Express, Discover, JBC, Master Card in Visa.

Pri vpeljavi standarda v podjetje trgovca je najpomembnejše, da dobro definiramo obseg varovanja informacij. Podrobnejše zahteve so definirane v več kot 220 točkah standarda PCI DSS. Vse zahteve mora trgovec izpolnjevati na vseh napravah, po katerih se obdelujejo, hranijo ali prenašajo občutljivi kartični podatki. Te naprave tvorijo PCI obseg. V PCI obseg uvrščamo tako tehnološke kot procesne vire, npr. strojno opremo kot so mrežne naprave, strežniki, računalniki, POS terminali, potem tudi programsko opremo, npr. poslovne aplikacije, ki imajo dostop do občutljivih kartičnih podatkov ter dokumenti v elektronski obliki. V PCI obseg spadajo tudi dokumenti v fizični obliki, kjer so zapisani občutljivi kartični podatki.

Opredelitev PCI obsega predstavlja zahtevnejši del vpeljave standarda. Potrebno je identificirati lokacijo kartičnih podatkov; kje se podatki hranijo, kateri podatki se hranijo in ali je takšna hramba dovoljena in potrebna. Če ugotovimo, da podatki v poslovnem procesu niso potrebni, poslovni proces ustrezno spremenimo.

Bistveni cilji, ki jih želimo z izvedbo projekta doseči, so naslednji:

- posodobitev platforme prodajnih mest (POS terminalov),
- zagotovitev podpore za brezstično plačevanje (ang. *Near Field Communication*) in s tem manjši stroški transakcij,
- dvigniti nivo varnosti kartičnega poslovanja,
- izpolnitev zahtev izdajateljev kartic, ki preko bank, s katerimi imamo sklenjeno pogodbo za sprejem kartic, od nas zahtevajo, da v določenem roku dosežemo in dokažemo skladnost s standardom PCI DSS,
- pravočasna priprava na v prihodnosti verjetno še ostrejše zahteve s strani izdajateljev kartic ter zaščita poslovnih interesov,
- uvajanje dobrih praks, ki jih zahteva standard PCI DSS lahko uveljavimo tudi na segmentih informacijskega poslovanja, ki niso neposredno povezani s kartičnim poslovanjem. To bi prineslo boljšo varnost informacijskega sistema kot celote in odpravo nekaterih slabosti, na katere so opozarjale že določene revizije v preteklosti.

Izzivi za trgovca so veliki, saj so potrebne velike spremembe, tako tehnološkega dela kot tudi procesnega. Spremeniti bo potrebno dostikrat brezbrižen pogled na varnost pri ljudeh. Na varnost ne smemo gledati kot na nepotreben strošek. Potrebno bo prilagoditi poslovne procese, da bodo skladni z varnostno politiko, ki jo zahteva standard PCI DSS.

3.1 Možni pristopi k rešitvi

Ker je izpolnjevanje zahtev na večjem številu naprav drago in časovno zelo zahtevno, veliko je rednih administrativnih in vzdrževalnih postopkov, je prvi korak pri reševanju te problematike omejevanje PCI obsega. Manj kot je naprav v PCI obsegu, manj virov je potrebnih za njihovo redno vzdrževanje. Z omejitvijo, kje se kartični podatki v organizaciji pojavljajo, zmanjšamo možne kršitve varnosti. Ker so zahteve PCI DSS obsežne in komplicirane, organizacije ves čas iščejo nove načine za zmanjšanje PCI obsega.

Manjši kot je PCI obseg, manj zahtev je potrebno izpolniti, ker nekatere ne pridejo v poštev. Manj zahtev pomeni manj dokumentacije ter nižje stroške pri testiranju in vzdrževanju skladnosti. Avtorji člankov in strokovna literatura [9–11, 21, 23] naštevajo različne načine, kako zmanjšati PCI obseg. Najpogosteje

omenjeni načini zmanjševanja PCI obsega so v podrobneje opisani v sledečih podpoglavjih:

- konsolidacija sistema,
- tokenizacija,
- najem zunanjega ponudnika storitve,
- segmentacija omrežja,
- šifriranje podatkov takoj ob zajemu.

3.1.1 Konsolidacija sistema

Konsolidacija sistema pomeni preureditev sistema na tak način, da izločimo kartične podatke iz tistih delov sistema, kjer niso nujno potrebni za izvajanje poslovanja. Potrebno je uskladiti programsko kodo ter jo na novo zasnovati na način, da ne uporablja občutljivih kartičnih podatkov, če jih ne potrebuje. S tem zmanjšamo kartično okolje in posledično PCI obseg. Zahteve standarda bi tako vpeljali na tistih napravah in virih, za katere smo določili, da so v PCI obsegu. To bi le minimalno zmanjšalo PCI obseg. Kot prednost rešitve lahko smatramo veliko varnost sistema, saj v PCI obsegu ostane velika množica naprav in virov. Če so ti varni, potem je celoten sistem varen.

Slabost te rešitve je, da bi zahtevala velike finančne in človeške vire zaradi velikega števila naprav in procesov, ki bi ostali v PCI obsegu. Tudi testiranje skladnosti, če vse v PCI obsegu zadošča 12 zahtevam in več kot 220 podzahtevam, bi bil drag in dolgotrajen proces. Še bolj problematično bi bilo kasnejše vzdrževanje takega sistema, saj bi obsežni administrativni postopki dokazovanja skladnosti s standardom, ki jih je treba izvajati periodično, zahtevali dodatno zaposlovanje za ta namen.

3.1.2 Tokenizacija

Tokenizacija (ang.: *Tokenization*) [23] predstavlja zamenjavo občutljivih kartičnih podatkov, v tem primeru PAN številke, z nadomestnim enoličnim podatkom podobnih lastnosti, kot je prikazano v tabeli 3.1. Namesto da se PAN številka zares pojavlja v podatkovnih bazah ali transakcijah, se uporabi žeton. Žeton je sklic oziroma referenca do originalnega podatka. Če pride do vdora

v bazo ali podatkovno transakcijo v okolju, bo nepooblaščena oseba prišla do žetona, a ta bo brez koristi, saj ne nosi dejanske informacije, je le sklic na izvorni podatek. Izvorni podatki pa se hranijo zgolj v močno zaščitenih podatkovnih trezorjih (ang.: *data vault*), ki se nahajajo v okolju trgovca ali pa v okolju ponudnika tokenizacije TSP (ang.: *tokenization service provider*).

PAN številka	**Žeton**	**Opis žetona**
3124 005917 23387	7aF1Zx118523mw4cwl5x2	Žeton je sestavljen iz alfanumeričnih znakov
4959 0059 0172 3389	729129118523184663129	Žeton je sestavljen iz numeričnih znakov
5994 0059 0172 3383	599400x18523mw4cw3383	Žeton je sestavljen iz odrezane PAN številke (prvih 6 številk in zadnje 4), vmesne številke pa nadomestijo alfanumerični znaki

Tabela 3.1: Primeri žetonov, ki nastanejo s tokenizacijo.

Glavna prednost tokenizacije je, da jo lahko uvedemo brez velikih posegov v obstoječ sistem. Aplikacije in naprave lahko normalno naprej delajo z žetoni, ker so podobni PAN številkam. V primeru lastne tokenizacije moramo v sistem dograditi le funkcionalnost za šifriranje in dešifriranje. Delo z žetoni namesto s PAN številkami pomaga zmanjšati okolje, kjer se občutljivi kartični podatki obdelujejo. Posledično je lažje implementirati zahteve standarda v podjetje, saj so tisti deli sistema, ki nimajo dostopa do podatkov v čisti obliki, izvzeti iz PCI obsega. Ta pristop bi ob vpeljavi zahteval vire, ki so primerljivi tistimi v prej omenjenem pristopu. Vzdrževanje sistema bi bilo sicer nekoliko enostavnejše in cenejše, a ne bistveno. Še vedno pa bi morali vpeljati in vzdrževati vse zahtevane postopke, le da na manjšem številu naprav.

3.1.3 Najem zunanjega ponudnika storitve

Najem zunanjega ponudnika storitve je zelo učinkovit način zmanjšanja PCI obsega, saj lahko kartične podatke na tak način popolnoma izločimo iz poslovnega okolja trgovca [11]. Ponudnik storitve nudi procesiranje kartičnih transakcij in hranjenje občutljivih kartičnih podatkov. Ponudnik storitve mora biti seveda skladen s PCI DSS standardom, drugače ta rešitev ne pride v poštev. Z njim sklenemo pogodbo, da v podjetje trgovca vpelje svoj sistem in storitve, potrebne za izvajanje kartičnih transakcij. Ponudnik je ponavadi banka, s katero sklenemo pogodbo o uporabi in najemu njihovih POS terminalov. Izmenjava podatkov se vrši preko POS terminala, ki je nameščen na prodajnem mestu trgovca in je last banke ponudnice storitve, do osrednjega računalnika v

banki izdajateljici kartic. Izmenjava podatkov poteka preko javnega omrežja po varni povezavi, občutljivi kartični podatki tako nimajo stika s poslovnim okoljem trgovca.

Prednost te rešitve je, da občutljive kartične podatke popolnoma izločimo iz poslovnega okolja trgovca, saj ves plačilni promet in podatke prepustimo banki ponudnici storitve. Kar pomeni, da v PCI obsegu ostane le osebje na prodajnem mestu, ki rokuje s samimi bančnimi karticami. To pa je ena od komponent, ki jih nikakor ne moremo izločiti iz PCI območja. Vpeljava standarda bi bila v primeru izbire te rešitve enostavna. Toda tudi če najamemo zunanjega ponudnika storitve, je naša dolžnost da spremljamo ponudnika in njegovo skladnost s standardom. Kar vseeno zahteva veliko manj truda, kot če ponudnika nebi najeli.

Slabost rešitve pa je njena neprilagodljivost. POS terminali, ki jih banke dajejo v najem, so narejeni le za procesiranje bančnih kartic. Prilagoditve aplikacije na POS terminalu za procesiranje ostalih plačilnih kartic, banke ponudnice storitve zelo drago zaračunajo ali pa te možnosti sploh ne nudijo. Druga slabost je, da trgovec sklene pogodbo za procesiranje transakcij z banko ponudnico storitve, kar pomeni, da je potrebno v primeru menjave banke zamenjati tudi celotno POS arhitekturo.

3.1.4 Segmentacija omrežja

S segmentacijo omrežja lahko dosežemo, da je omrežje, kjer se občutljivi kartični podatki prenašajo, ločeno od omrežja, kjer se prenašajo ostali podatki potrebni za poslovanje [10]. Brez segmentacije oziroma izolacije omrežja je v PCI obsegu celotno omrežje. Segmentacijo omrežja lahko dosežemo na več načinov, s kontrolami fizične ali logične narave. Te kontrole lahko vsebujejo požarne pregrade, navidezna lokalna omrežja VLAN (ang.: *Virtual Local Area Network*), dve ali več popolnoma ločenih omrežij, ipd. Največkrat uporabljena možnost so požarne pregrade ali VLAN, zato pa potrebujemo močne omejitve na napravah, da lahko ločimo omrežje, ki ni v PCI obsegu od omrežja, ki je v PCI obsegu.

Pri tem načinu je potrebno konstantno skrbeti za nadzor prometa v omrežju, nadzorovati naprave, ki izvajajo kontrole nad prometom v omrežju ter vzdrževati omejitve na napravah. PCI območje se sicer zmanjša, kar pomeni, da bi vseeno morali vpeljati vse zahteve PCI DSS, le da na manjšem številu naprav.

3.1.5 Šifriranje podatkov takoj ob zajemu

Šifriranje občutljivih kartičnih podatkov takoj ob zajemu je možna rešitev za zmanjšanje PCI območja [9]. Za to je seveda potrebno uporabiti močne šifrirne algoritme. Ker se da šifrirane podatke dešifrirati, če pridobimo pravi ključ, ostanejo tudi šifrirani podatki v PCI obsegu. Edina možnost, da šifrirani podatki niso v PCI obsegu je, če podjetje nima dostopa niti do ključev niti do procesa, kjer se občutljivi kartični podatki šifrirajo, niti dostopa do okolja, kjer se nahajajo podatki v čisti obliki. Pristop temelji na šifriranju občutljivih kartičnih podatkov takoj ob zajemu in njihovo dešifriranje izven trgovčevega komunikacijskega omrežja. Pomemben pogoj, da trgovec lahko uporabi ta pristop, je izvedba na način, pri katerem šifrirni ključi trgovcu niso dostopni oz. znani. S tem je zagotovljeno, da trgovec (ali kdorkoli bi vdrl v njegovo komunikacijsko omrežje) nima možnosti, da bi lahko šifrirane kartične podatke dešifriral in pridobil kartične podatke v berljivi obliki. Zaradi tega je potrebno med trgovca in procesni center vpeljuje še tretjo stranko in sicer ponudnika varnostne storitve (ang.: *Security Solution Provider*). Ta je zadolžen za upravljanje z šifrirnimi ključi, certifikati in ostalimi uporabljenimi varnostnimi mehanizmi.

Če se podatki res šifrirajo takoj ob zajemu, torej na točki, ko kupec vstavi ali potegne bančno kartico čez POS terminal in dešifrirajo pri ponudniku varnostne rešitve, se izognemo temu, da se po omrežju pretakajo podatki v čisti obliki. Tako tudi ni možnosti, da so v okolju trgovca shranjeni podatki v čisti obliki, kar še dodatno zmanjša število zahtev, ki jih moramo izpolniti. Če pride do vdora v sistem, so podatki o karticah za napadalca neuporabni. Ker se po okolju trgovca prenašajo le šifrirani podatki, se na tak način PCI obseg omeji na minimum, saj v PCI obsegu ostane le POS terminal in prodajalec. Prodajalec je en od elementov, ki ga nikakor ne moremo izločiti iz PCI obsega. Podjetje mora še vedno izpolnjevati zahteve PCI DSS, vendar je z nekaterimi zahtevami skladen avtomatsko, saj se po omrežju ne pretakajo občutljivi kartični podatki. Taka rešitev sicer zahteva vpeljavo zunanjega ponudnika varnostne rešitve.

Poglavje 4

Izvedba projekta

V sledečem poglavju bomo opisali, na kakšen način smo se lotili vpeljave standarda PCI DSS v podjetje velikega trgovca. Razložili bomo, katera izmed rešitev je bila optimalna izbira za podjetje. Opisali bomo, katere dele sistema smo morali sami razviti in implementirati ter katere dele smo kupili od zunanjih ponudnikov. Na koncu bomo pregledali, kaj v podjetju po implementaciji rešitve spada v PCI obseg in katerim zahtevam bomo morali zadostiti.

4.1 Optimalna rešitev

Optimalna rešitev je tista, s katero lahko dosežemo minimalni PCI obseg. Manjši PCI obseg pomeni nižje stroške pri vpeljavi standarda v podjetje, vzdrževanju naprav ter manj dokumentacije pri vsakoletnem ocenjevanju in dokazovanju skladnosti. Pri izbiri rešitve za vpeljavo standarda je bilo potrebno tudi sodelovanje z izbranim zunanjim kvalificiranim ocenjevalcem. Tudi če se neka rešitev trgovcu zdi popolna, jo zunanji kvalificirani ocenjevalec lahko zavrne. Veliko je odvisno od njegove subjektivne presoje.

V podjetju trgovca smo izbrali rešitev »Šifriranje podatkov takoj ob zajemu«, ki jo je potrdil tudi zunanji kvalificirani ocenjevalec. K lažji izbiri optimalne rešitve je močno pripomoglo eno izmed pogosto zastavljenih vprašanj na uradni spletni strani Sveta PCI SCC. Gre za vprašanje »*Frequently Asked Question - Article Number: 1086*« [9], ki se glasi: »Ali so šifrirani podatki o imetniku kartice v PCI območju?«. Uradni odgovor Sveta PCI SSC je, da je šifriranje občutljivih podatkov sprejemljiva metoda, da se zagotovi skladnost z zahtevo

3.4 [10]. Zahteva 3.4 narekuje naslednje: »Kjer je PAN številka shranjena, mora biti shranjena v neberljivi obliki«. Za šifriranje občutljivih kartičnih podatkov je potrebno izbrati močne šifrirne algoritme. Ker je šifrirane podatke možno dešifrirati, če imamo pravi ključ, ostanejo šifrirani podatki v PCI obsegu. Obstaja pa možnost, da šifrirane podatke izločimo iz PCI obsega. To je možno samo v primeru, da trgovec nima dostopa do občutljivih kartičnih podatkov v čisti obliki. Prav tako trgovec ne sme imeti dostopa do procesa, kjer se občutljivi kartični podatki šifrirajo. Trgovec ne sme imeti dostopa do ključev, s katerimi bi šifrirane podatke lahko dešifriral. Ključi za šifriranje in dešifriranje torej ne smejo obstajati v trgovčevem poslovnem, komunikacijskem okolju. Noben poslovni proces in nihče od zaposlenih ne sme imeti stika z okoljem, kjer se ključi nahajajo. Niti ne sme imeti možnosti, da bi lahko kakorkoli dostopal do okolja, kjer se ključi nahajajo.

Izbrana rešitev zahteva vpeljavo zunanjega ponudnika varnostne rešitve, ki skrbi za upravljanje s šifrirnimi ključi. Okolje, kjer se občutljivi kartični podatki šifrirajo oziroma dešifrirajo ter sistem, ki skrbi za upravljanje s šifrirnimi ključi, spada v PCI obseg. Torej mora tudi okolje ponudnika varnostne rešitve biti skladno s standardom PCI DSS. Z izbrano rešitvijo smo dosegli, da v trgovčev PCI obseg spada samo POS terminal in prodajalec. Tudi prodajalec namreč vidi celotno PAN številko na kartici. Trgovec mora v poročilu skladnosti zagotoviti, da je ponudnik varnostne rešitve skladen s standardom, ponudnik pa mora to dokazati trgovcu.

Kot rečeno, je način izvedbe projekta odvisen od mnenja zunanjega kvalificiranega ocenjevalca. Kvalificirani ocenjevalec mora potrditi predlagano izvedbo že pred začetkom dejanske izvedbe projekta. Drugače nas lahko v poročilu o skladnosti oceni kot neskladne s standardom PCI DSS. Za uspešno potrditev skladnosti mora sistem zadoščati naslednjim trditvam:

- občutljivi kartični podatki se procesirajo na POS terminalu in se takoj ob zajemu šifrirajo,
- občutljivi kartični podatki se lahko dešifrirajo samo pri izbranem ponudniku varnostne rešitve in nikjer drugje,
- občutljivi kartični podatki se v trgovčevem okolju pojavljajo samo na POS terminalu in nikjer drugje, POS terminal pa je overjen s strani Sveta PCI SSC.

Za izvedbo rešitve smo morali razviti naslednje komponente, ki so podrobneje opisane v sledečih poglavjih:

- razvoj aplikacije, ki teče na POS terminalu in pošilja šifrirane kartične podatke na POS strežnik,
- razvoj Osrednje dekripcijske naprave, ki skrbi za dešifriranje kartičnih podatkov in pošiljanje podatkov v čisti obliki na avtorizacijske strežnike.

4.2 POS terminali

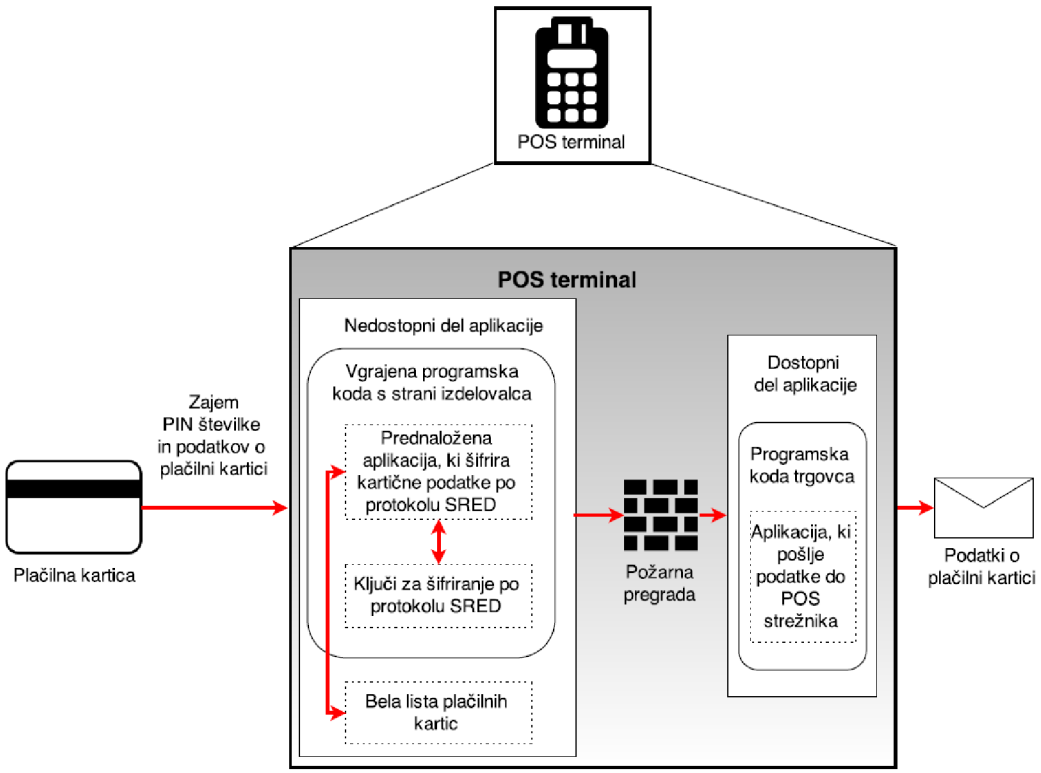
POS terminal je elektronski čitalec na prodajnem mestu, ki je namenjen elektronskemu prenosu podatkov med prodajnim mestom, procesnim centrom in banko izdajateljico kartice pri plačilni transakciji z bančno kartico [13].

Izbrana rešitev se v veliki meri navezuje na POS terminale. Obstoječi POS terminali niso več zadoščali zahtevam kartičnih in varnostih institucij. Prav tako so bili stari ter dotrajani, kar je povzročalo velike stroške vzdrževanja. Za izvedbo projekta je bilo potrebno poiskati nove, ustrezne POS terminale, ki omogočajo izpeljavo izbrane rešitve. POS terminal mora biti certificiran, da iz njega pod nobenim pogojem ne morejo priti podatki v čisti obliki. To pa je tudi ena od zahtev standarda PCI PTS. Obrnili smo se na spletno stran Sveta PCI SSC, kjer so naštete naprave, ki so skladne s standardom PCI PTS [6].

Glavne zahteve za nove POS terminale, ki so podrobneje razložene v nadaljevanju, so sledeče:

- skladnost strojne opreme s standardom PCI PTS,
- možnost bele liste (ang.: *whitelist*) plačilnih kartic,
- odprtokodna programska oprema in možnost nalaganja posodobitev programske opreme na daljavo,
- podpora za oddaljeno nalaganje šifrirnih ključev,
- sistem za upravljanje s terminali TMS (ang.: *Terminal Management System*),
- možnost dograditve za brez-kontaktno plačevanje s kartico.

Izbran je bil POS terminal Yomani podjetja Atos Worldline [8], ki ima zastopstvo tudi v Sloveniji. Ta terminal je skladen z vsemi naštetimi zahtevami. Napravo je Svet PCI SSD potrdil kot skladno s standardom PCI PTS, kar pomeni da pokrije tudi nekatere zahteve standarda PCI DSS.



Slika 4.1: Arhitektura POS terminala.

Glavna prednost te naprave je, da je arhitektura POS terminala taka, da na njem lahko deluje več aplikacij naenkrat [3]. Prva aplikacija je pred-naložena na POS terminalu in je ne moremo spreminjati. Ta aplikacija poskrbi za to, da se podatki takoj ob zajemu šifrirajo s protokolom SRED (ang.: *Secure Reading and Exchange of Data*, v nadaljevanju: SRED) [13] in spada v okolje ponudnika varnostne rešitve. Druga aplikacija na POS terminalu spada v okolje trgovca in jo lahko spreminjamo. Okvirno arhitekturo POS terminala si lahko ogledamo na sliki 4.1.

Aplikacija v trgovčevem okolju nima dostopa do podatkov aplikacije, ki je v okolju ponudnika varnostne rešitve, čeprav se nahaja na isti napravi. Za to poskrbijo varnosti mehanizmi in požarne pregrade, ki so vgrajene v napravo. Podatki iz prve aplikacije ne morejo priti v drugo aplikacijo v čisti obliki, izmenjava podatkov pa poteka enosmerno. Aplikacija, ki vsebuje simetrične ključe za šifriranje podatkov po protokolu SRED, je po zagotovilih izdelovalca

povsem ločena od ostalih aplikacij, ki se izvajajo na POS terminalu.

V podjetju trgovca sprejemamo tudi plačilne kartice zvestobe za fizične osebe, poslovne kartice zvestobe za pravne osebe in ostale mednarodne plačilne kartice (npr. UTA in DKV kartice). Teh kartic ne izdajajo banke izdajateljice kartic, ki sestavljajo Svet PCI SSC. Te kartice se torej ne avtorizirajo v banki ali procesnem centru, temveč preko osrednjega strežnika trgovca. Omenjene kartice torej ne padejo pod zahteve in nadzorstva standarda PCI DSS, občutljivih kartičnih podatkov teh kartic pa ni potrebno šifrirati. Aplikacija na POS terminalu, ki skrbi za šifriranje občutljivih kartičnih podatkov, lahko podatke teh kartic preda naprej v čisti obliki. Te kartice je potrebno dati na belo listo, ki jo mora potrditi ponudnik varnostne rešitve. Čeprav podatkov kartic z bele liste ni potrebno šifrirati v skladu z zahtevami standarda PCI DSS, so podatki o imetnikih kartic zaščiteni v skladu z zakonom o varovanju osebnih podatkov.

POS terminali so certificirani v skladu s standardom PCI PTS in podatki v čisti obliki nikakor ne morejo priti iz naprave. Aplikacija za šifriranje, ki teče na POS terminalu, spada pod zahteve PCI PTS in je prav tako skladna s standardom. Druga aplikacija, ki jo lahko naši razvijalci spreminjajo glede na poslovne potrebe, npr. za povezavo s POS strežnikom, pa ne spada pod zahteve PCI DSS, saj ne procesira, hrani ali pošilja občutljivih kartičnih podatkov. Ker pa se strojna oprema, torej POS terminal, še vedno nahaja v poslovnem okolju trgovca, se za POS terminal smatra, da je v PCI obsegu. Trgovec mora sam poskrbeti za posodobitve programske opreme, nameščanje popravkov, protivirusno zaščito, fizično preveriti POS terminale, da ni na njih kakšnih nedovoljenih posegov, ipd.

4.3 Osrednja dekripcijska naprava

Ena izmed glavnih komponent sistema za vzpostavitev skladnosti s standardom PCI DSS je Osrednja dekripcijska naprava. Osrednja dekripcijska naprava se ne nahaja v okolju trgovca, temveč v okolju ponudnika varnostne rešitve, ki je obenem tudi procesni center. Z Osrednjo dekripcijsko napravo upravlja ponudnik varnostne rešitve, ker trgovec ne sme imeti dostopa niti do okolja, kjer se podatki šifrirajo, kaj šele do naprave, ki skrbi za šifriranje in dešifriranje.

Osrednjo dekripcijsko napravo je možno vzpostaviti na dva načina. Prvi način je kupljena rešitev (s prilagoditvijo), drugi način pa je razvoj lastne rešitve. Ocenili smo, da je lastna rešitev stroškovno bolj optimalna in ponuja večjo

prilagodljivost glede spreminjanja v prihodnje. Res pa je, da je lastna rešitev zahtevala nekaj več lastnih virov pri razvoju in vzpostavitvi. Tudi vzdrževanje v prihodnje bo zahtevalo lastne vire.

V okolje ponudnika varnostne rešitve smo postavili dve Osrednji dekripcijski napravi, primarno in sekundarno. Posamezno Osrednjo dekripcijsko napravo napravo sestavljata dva dela, kot je prikazano na spodnji sliki 4.2:

- varni protokolni pretvornik SPC (ang.: *Secure Protocol Converter*, v nadaljevanju: SPC),
- varni strojni modul HSM (ang.: *Hardware Security Modul*, v nadaljevanju: HSM).

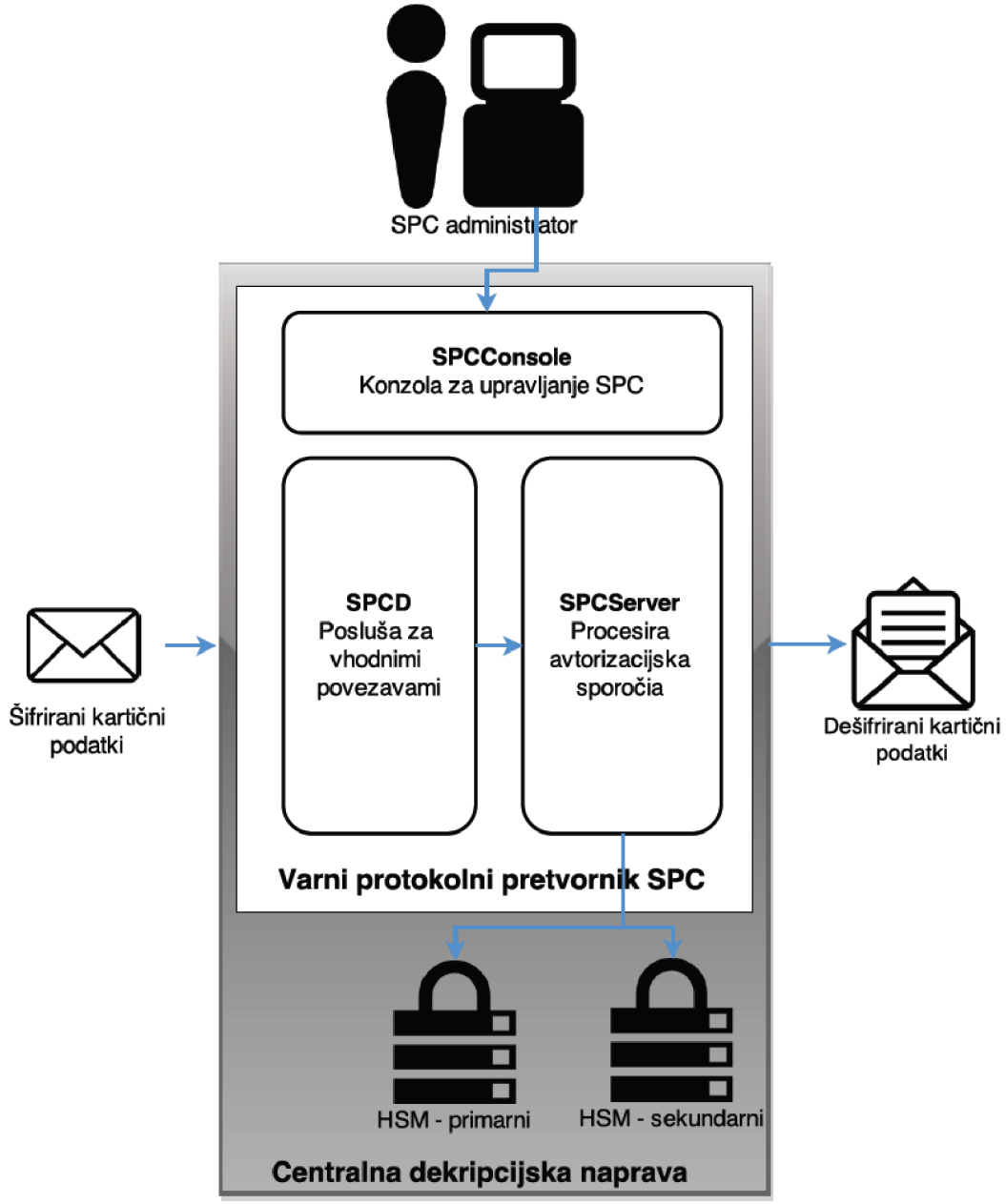
4.3.1 Varni protokolni pretvornik SPC

Protokolni pretvornik je naprava, ki skrbi za pretvorbo protokolov med napravami in omrežji. Zagotavlja transformacijo podatkov med različnimi okolji in tako omogoča možnost komunikacije [25].

Varni protokolni pretvornik oz. SPC je podrobneje narisan na sliki 4.2, umestitev v sistem pa vidimo na sliki 4.3. SPC predstavlja povezavo med POS terminalom na strani trgovca in avtorizacijskim strežnikom na strani procesnega centra. S POS terminala pride po varni povezavi zahteva za avtorizacijo kartične transakcije. SPC podatke dešifrira s pomočjo varnega strojnega modula HSM. Podatke v čisti obliki pošlje avtorizacijskemu strežniku. Ko dobi povratno sporočilo od avtorizacijskega strežnika, podatke v čisti obliki ponovno šifrira in jih pošlje tistemu POS terminalu, ki je zahtevo poslal.

Ko SPC dobi zahtevo za povezavo preko določenih vrat, se zgodijo naslednji koraki [1]:

1. SPC sprejme šifrirano sporočilo od prodajnega terminala preko SSL povezave.
2. Pregleda sporočilo in poišče tisti del sporočila, ki je šifriran.
3. Šifriran del sporočila pošlje po varni povezavi SSL v HSM napravo.
4. Sprejme dešifrirano sporočilo po varni povezavi SSL od HSM naprave.
5. V originalnem sporočilu zamenja šifrirane podatke z dešifriranimi (npr. odrezano PAN številko s celotno PAN številko).



Slika 4.2: Komponenti Osrednje dekripcijske naprave: SPC in HSM.

6. Dešifrirano sporočilo pošlje po varni povezavi SSL na avtorizacijski strežnik.

7. Počaka na odgovor avtorizacijskega strežnika.
8. Sprejeti odgovor pregleda in če vsebuje občutljive kartične podatke, te zamenja z šifriranimi podatki.
9. SPC pošlje šifrirano sporočilo o odgovoru banke po varni povezavi SSL nazaj originalnemu klicatelju (POS terminalu).

SPC sestavljajo naslednje komponente, kot lahko vidimo na sliki 4.2:

- **SPCConsole - Konzola za upravljanje SPC:** Konzola za upravljanje SPC je terminal z grafičnim vmesnikom (ang.: *ncurses text-based*) [17]. S pomočjo konzole SPCConsole administrator upravlja z ostalimi komponentami SPC naprave (SPCD in SPCServer). Konzola se izvaja na SPC napravi z njo pa se je mogoče povezati preko SSH protokola za upravljanje računalnika na daljavo, ki uporablja simetrične ključe. Konzola SPCConsole omogoča administratorju pregled statusa komponent SPC, zagon in zaustavitev SPC procesov, pregled dnevnika (ang.: *log*), alarmov in statistike, omogočena je konfiguracija SPC.
- **SPCD - Poslušalec vhodnih povezav:** SPCD je strežniška komponenta (ang.: *superdaemon xinetd*) [20] v SPC napravi, ki zagotavlja sprejemanje povezav s POS terminalov na določenih vratih TCP (ang.: *Transmission Control Protocol*). Poslušalec SPCD je odgovoren za delegiranje vhodnih povezav instancam SPCServer-ja, ki nato procesira vhodne zahteve za avtorizacije transakcij.
- **SPCServer - Strežnik za procesiranje avtorizacijskih sporočil:** SPCServer je strežniški proces s kratko življenjsko dobo (ang.: *short-lived server process*) kar pomeni, da se podatki o procesu ne shranjujejo. Tako je zagotovljena večja hitrost delovanja. SPCServer je zadolžen za procesiranje zahtev za avtorizacije transakcij.

SPC za zaščito podatkov podpira SSL/TLS tehnologijo (ang.: *Secure Sockets Layer/Transport Layer Security*, v nadaljevanju SSL/TLS). SPC administrator certfikate ureja preko konzole za upravljanje SPC. SPC vsebuje več ločenih SSL/TLS certifikatov za povezavo in avtentikacijo med večimi točkami, kar je prikazano na sliki 4.3:

- med POS terminalom in SPC napravo,
- med HSM napravo in SPC napravo,
- med SPC napravo in avtorizacijskimi strežniki Bankarta.

4.3.2 Varni strojni modul HSM

Varni strojni modul oz. HSM je naprava, ki omogoča zanesljivo hranjenje šifrirnih ključev in digitalnih potrdil pred fizičnimi in digitalnimi napadi [24]. V HSM napravi se nahajajo šifrirni ključi. HSM vsebuje kontrole, ki v primeru nedovoljenih posegov v napravo shranijo dokaze o napadu. V primeru fizičnega nedovoljenega posega pa se šifrirni ključi samodejno izbrišejo.

SPC je povezan z dvema HSM napravama, primarno in sekundarno HSM napravo. Oba HSM modula imata naloženo isto množico ključev zaradi redundance. Če prvi modul preneha delovati, drugi modul prevzame njegove naloge. Način za preklapljanje med HSM napravama v primeru izpada se imenuje nadomestni način delovanja (ang.: *fail-over*). SPC v primeru izpada primarne HSM naprave neopazno in nemoteno preklopi na sekundarno HSM napravo. Ključi, ki so shranjeni v HSM napravi, so simetrični šifrirni ključi. Občutljivi kartični podatki se s simetričnim ključem šifrirajo v POS terminalu, potem pa se v SPC s pomočjo HSM dešifrirajo. Ti ključi so DUKPT 3DES [22, 26] ključi.

HSM smo kupili od istega ponudnika kot POS terminale, saj obe napravi uporabljata iste simetrične ključe za šifriranje podatkov. Šifrirne ključe v POS terminale in HMS naprave vstavi izdelovalec, POS terminale potem preda trgovcu, HSM naprave pa ponudniku varnostne rešitve. Ko ponudnik varnostne rešitve HSM poveže na SPC, lahko SPC začne s dešifriranjem podatkov, ki jih dobi od POS terminalov.

4.4 Ponudnik varnostne rešitve

Zelo pomemben del izbrane rešitve za vpeljavo skladnosti s PCI DSS je ponudnik varnostne rešitve (ang.: *solution provider*). Ponudnik varnostne rešitve je poslovni subjekt, ki izvaja storitve procesiranja, hranjenja ali pošiljanja kartičnih podatkov namesto neke druge organizacije [12]. Okolje ponudnika varnostne rešitve mora biti skladno s standardom PCI DSS.

Vloga ponudnika varnostne rešitve oziroma njegove glavne aktivnosti so:

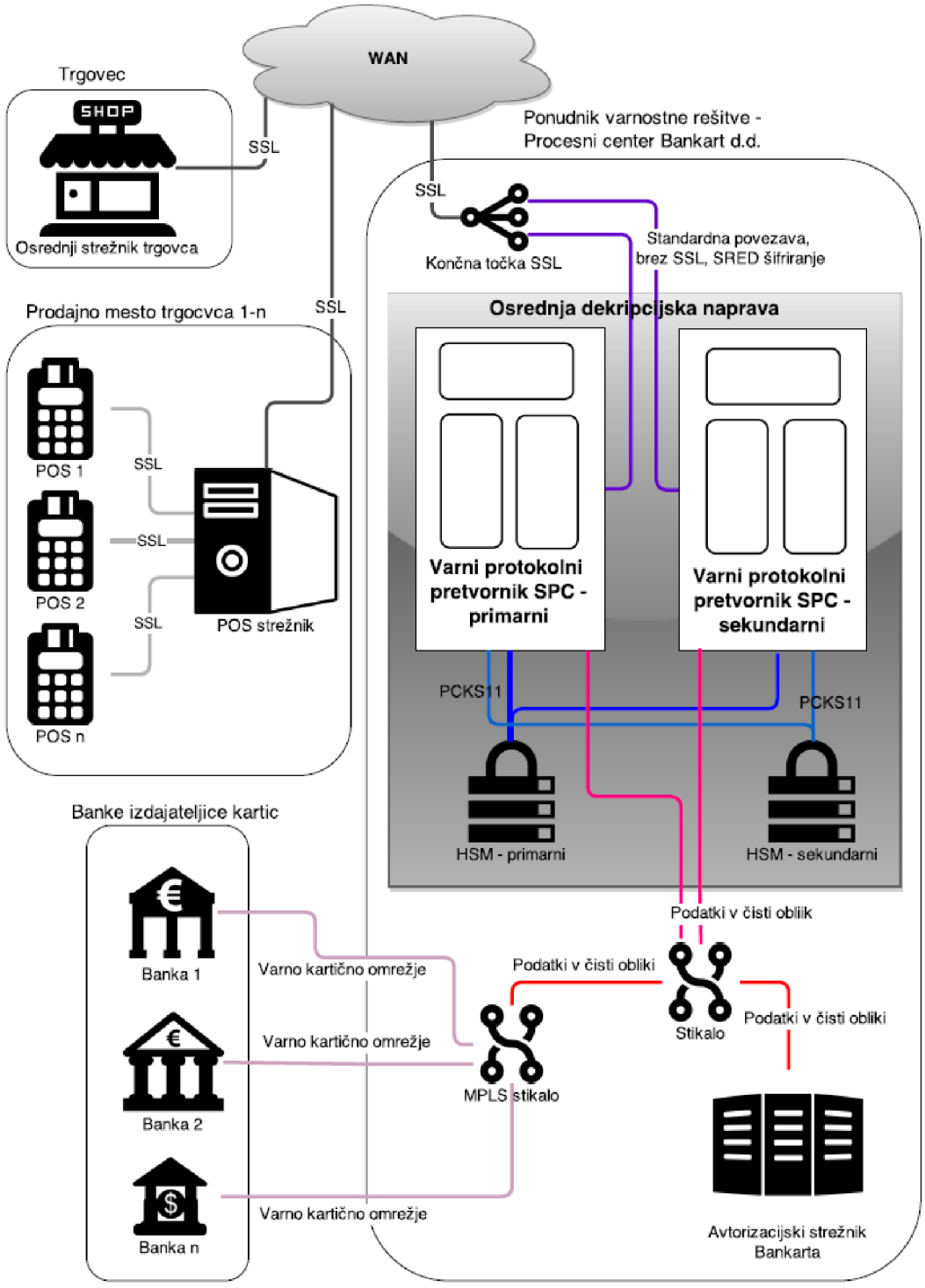
- upravljanje s ključi, ki se uporabljajo za šifriranje in dešifriranje,
- nalaganje ključev na naprave, ki sodelujejo v poteku kartične transakcije,

- upravljanje z Osrednjo dekripcijsko napravo,
- skrb za izvajanje vseh aktivnosti na Osrednji dekripcijski napravi, ki jih standard PCI DSS zahteva za naprave v PCI obsegu.

Slika 4.3 prikazuje, kako izgleda sistem ponudnika varnostne rešitve po implementaciji Osrednje dekripcijske naprave v njegovo okolje. Na prodajnih mestih se nahajajo POS terminali. Na vsakem prodajnem mestu sta vsaj dva POS terminala, na večjih prodajnih mestih pa tudi do 10 POS terminalov. Vsak izmed POS terminalov je povezan s POS strežnikom. Na vsakem prodajnem mestu je en POS strežnik. POS strežnik preko varne internetne povezave SSL pošlje šifrirane kartične podatke do ponudnika varnostne rešitve. Pri ponudniku varnostne rešitve se nahaja Osrednja dekripcijska naprava. Ko se s pomočjo le-te šifrirani kartični podatki dešifrirajo, se podatki v čisti pošljejo do bank. Banka zahtevo za avtorizacijo transakcije zavrne ali odobri in odgovor pošlje nazaj do ponudnika varnostne rešitve, ta pa preko POS strežnika do POS terminala, ki je sprožil zahtevo za transakcijo. Na sliki vidimo tudi katere vrste šifriranja podatkov in različne vrste protokolov za varne povezave se uporabljajo med komponentami sistema.

Vlogo ponudnikov takšnih storitev lahko igrajo procesni centri ali pa za to specializirana podjetja. Ker posredovanje vsake kartične transakcije nekaj stane, je bolje imeti čim manj posrednikov med trgovcem in banko. Procesni center je poslovni subjekt, s katerim imajo banke sklenjene pogodbe za obdelavo podatkov plačilnih transakcij s karticami [2]. Procesni center ima direktno povezavo do visoko-razpoložljivega transportnega omrežja MPLS TCP/IP (ang.: *Multiprotocol Label Switching*) [18], ki omogoča povezanost z bankami na varen in hiter način. Visoka razpoložljivost delovanja komunikacijskih povezav se zagotavlja s podvojeno strojno opremo in podvojenimi omrežnimi povezavami preko različnih ponudnikov telekomunikacijskih storitev. Trgovec tako pošilja zahteve za kartične transakcije procesnemu centru, nazaj pa dobi informacijo o odobreni ali zavrnjeni transakciji. Prednost procesnega centra je, da trgovec pošilja kartične transakcije samo na eno lokacijo in sicer do procesnega centra. Procesni center pa poskrbi, da se kartične transakcije pošljejo naprej do različnih bank.

Izbira ponudnika varnostne rešitve ni bila težka naloga. Podjetje že ima sklenjeno pogodbo za procesiranje kartičnih transakcij s procesnim centrom Bankart d.o.o. Z njimi smo sklenili dodatno pogodbo, da postanejo še naš ponudnik varnostne rešitve. S certifikatom so nam dokazali, da je njihovo okolje skladno z zahtevami standarda PCI DSS. Slika 4.3 prikazuje elemente sistema, ki smo



Slika 4.3: Slika prikazuje arhitekturo podjetja Bankart z implementirano Osrednjo dekripcijsko napravo. Iz slike je razvidno, kateri protokoli se uporabljajo za varne povezave med komponentami sistema in katere algoritmi za šifriranje podatkov so uporabljeni.

jih implementirali v okolju podjetja Bankart.

4.4.1 Prenos podatkov

Podatki o imetniku kartice se zajamejo na POS terminalu. Ali so podatki šifrirani in kam se pošljejo je odvisno od vrste plačilne kartice. Kot že omenjeno, je potrebno skladno s PCI DSS šifrirati samo tiste bančne kartice, ki jih izdajajo banke izdajateljice kartic, ki skupaj tvorijo Svet PCI SSC. V podjetju trgovca pa sprejemamo poleg bančnih kartic tudi druge vrste plačilnih kartic. Sem spadajo plačilne kartice zvestobe in plačilne kartice drugih trgovcev, s katerimi imamo sklenjeno pogodbo o sprejemanju njihovih kartic (mednarodne kartice npr. UTA in DKV kartice).

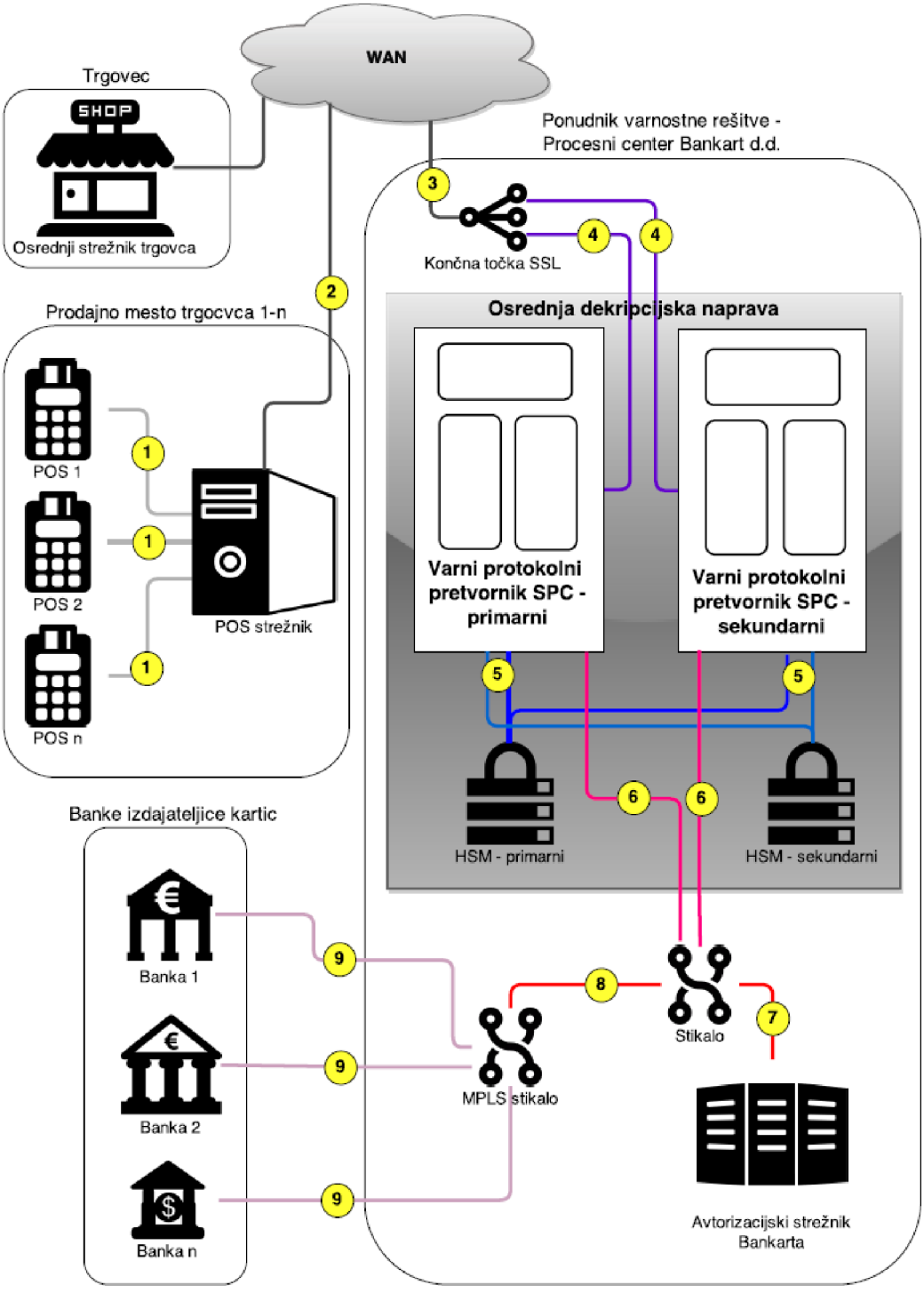
Na sliki 4.4 vidimo tok podatkov, ki se nanaša na bančno kartico, za katero veljajo zahteve standarda PCI DSS. S številkami od 1 do 9 so označeni koraki od zajema podatkov o imetniku kartice na POS terminalu do odobritve oz. zavrnitve zahteve za avtorizacijo transakcije s strani banke. Odgovor banke se po isti poti pošlje nazaj do POS terminala. Na sliki 4.3 lahko vidimo kateri varnostni protokoli so uporabljeni med različnimi komponentami sistema.

Na sliki 4.5 vidimo tok podatkov, ki se nanaša na plačilno kartico, za katero ne veljajo zahteve standarda PCI DSS. Ti tipi kartic so zapisani na beli listi, ki je vgrajena v vsak POS terminal. Če se tip kartice nahaja na beli listi, se podatki o kartici ne šifrirajo s SRED algoritmom. Podatki se po varni povezavi pošljejo do osrednjega strežnika trgovca. S številkami od 1 do 3 so označeni koraki od zajema podatkov o imetniku kartice na POS terminalu do odobritve oz. zavrnitve zahteve za avtorizacijo transakcije s strani trgovca. Odgovor trgovca se po isti poti pošlje nazaj do POS terminala.

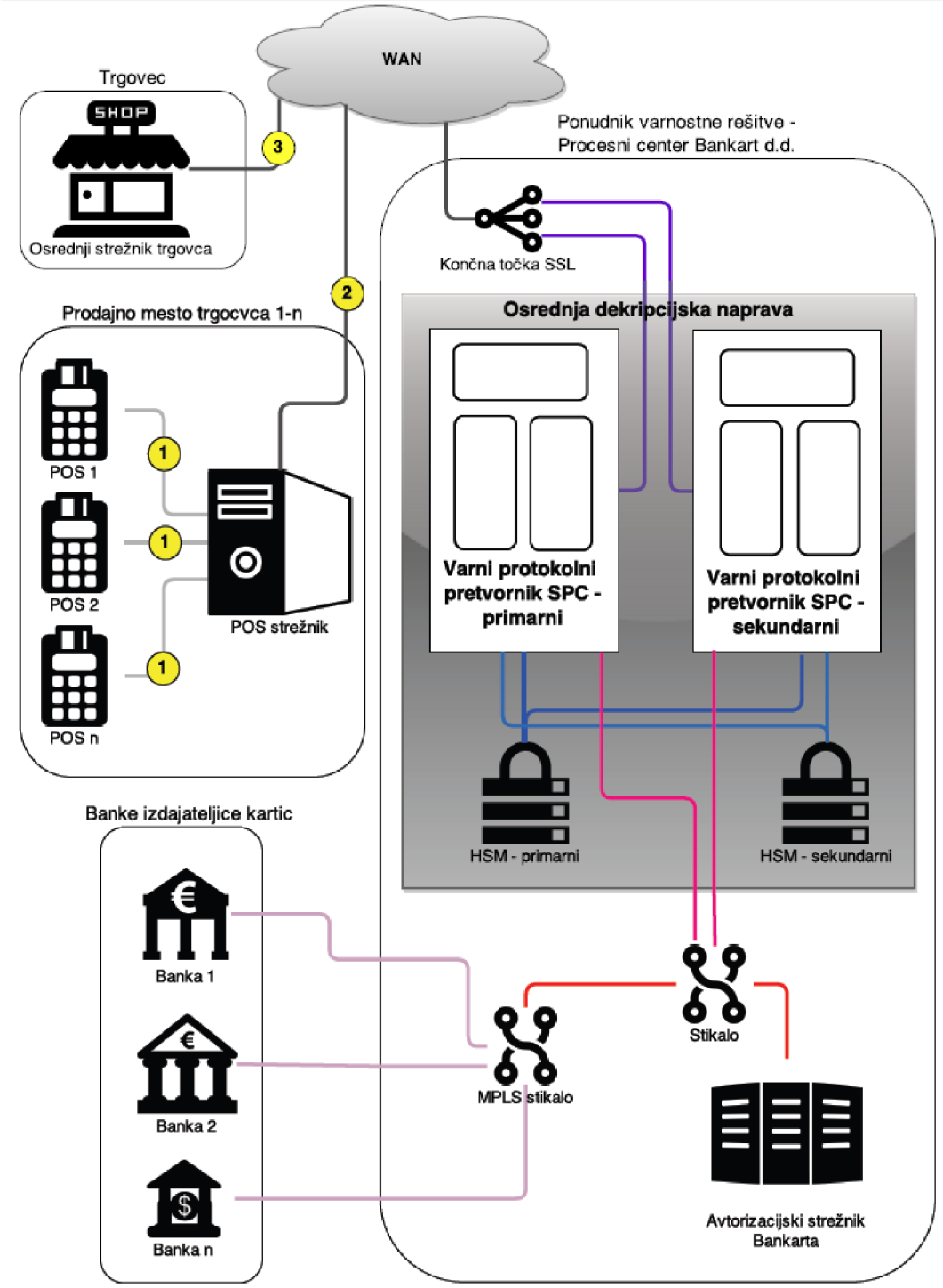
Če gre za plačilno kartico drugega trgovca, s katerim imamo sklenjeno pogodbo o sprejemanju njihovih kartic, se podatki o zahtevi za avtorizacijo transakcije pošljejo po varni povezavi do strežnika drugega trgovca. Odgovor o odobreni oz. zavrnjeni zahtevi se preko osrednjega strežnika trgovca pošlje nazaj do POS terminala.

4.4.2 Upravljanje s ključi

Ponudnik varnostne rešitve je dolžan opravljati s šifrirnimi ključi. Ključi so bili neposredno nameščeni na POS terminale že v tovarni, kjer so bili izdelani.



Slika 4.4: Arhitektura podjetja Bankart z implementirano Osrednjo dekripcijsko napravo. Na sliki je prikazan tok podatkov za avtorizacijo zahteve za transakcijo, izvedene z bančno kartico.



Slika 4.5: Arhitektura podjetja Bankart z implementirano Osrednjo dekripcijsko napravo. Na sliki je prikazan tok podatkov za avtorizacijo transakcije plačilne kartice, ki ne spada pod zahteve standarda PCI DSS.

Enako velja za ključe na HSM napravi. Toda v primeru, da je transakcija ogrožena in ključ prestrežen, je potrebno ključ v POS terminalu in HSM napravi zamenjati. Da ni potrebno za vsak ogrožen ključ iti na fizično lokacijo POS terminala in ga odnesti v varno okolje ponudnika varnostne rešitve ter nanj naložiti nove ključe, je na voljo sistem oddaljenega nalaganja ključev RKL (ang.: *Remote Key Loading*) [3], ki se vrši preko varne povezave čez javno omrežje. Sistem oddaljenega nalaganja ključev tako zniža stroške vzdrževanja, zveča varnost postopka nalaganja, pohitri cel postopek in je vsekakor bolj priročno.

4.5 PCI obseg v podjetju

PCI obseg v podjetju trgovca nam je uspelo drastično zmanjšati. V PCI obsegu ostane samo POS terminal, ker se na njem vrši šifriranje podatkov in se nahaja v trgovčevem okolju. V PCI obsegu trgovca je tudi osebje na prodajnih mestih, ki vsakodnevno rokuje s plačilnimi karticami in posledično vidi podatke o imetniku kartice. Zaradi zmanjšanja PCI obsega nam torej ni potrebno vpeljati vseh dvanajstih zahtev iz tabele 2.2 v podjetje. Nekatere zahteve za nas ne pridejo v poštev, ker se kartični podatki takoj ob zajemu šifrirajo.

Projekt vpeljave standarda PCI DSS v podjetje je še v fazi izvajanja. Zaenkrat je na 10-ih prodajnih mestih nameščeno 10 novih testnih POS terminalov, ostali terminali na prodajnih mesti so stari. Eden izmed začetnih ciljev je nova POS arhitektura na vseh prodajnih mestih. Kar pomeni približno 400 prodajnih mest v državah Slovenije, Hrvaške, Srbije, Črne Gore in Bosne in Hercegovine, torej okoli 1000 novih POS terminalov. To priča o tem, kako velik je ta projekt in kako časovno zahteven je. Poročila o skladnosti še nismo izpolnili, zato nas testiranje vseh zahtev in podzahtev še čaka.

Nekatere od zahtev iz tabele 2.2 pokrije certificiran POS terminal, ki je skladen s standardom PCI PTS. Kljub temu je odgovornost na strani trgovca, da poroča o skladnosti zahtev. Nekatere zahteve, ki ne pridejo v poštev za izvedbo so:

- **Zahteva 1: Vzpostavi in vzdržuj konfiguracijo požarne pregrade** - Razlog, da ta zahteva odpade je v tem, da je požarna pregrada že vgrajena v POS terminal in preprečuje stik podatkov v čisti obliki z okoljem trgovca.
- **Zahteva 3: Zavaruj shranjene podatke o imetniku kartice** - Od-

govornost hranjenja kartičnih podatkov je na strani ponudnika varnostne rešitve.

- **Zahteva 4: Šifriraj prenos kartičnih podatkov preko odprtih, javnih omrežij** - Za šifriranje kartičnih podatkov je zadolžen ponudnik varnostne rešitve, prav tako je zadolžen za varno pošiljanje podatkov.
- **Zahteva 9: Omeji fizični dostop do podatkov o imetnikih plačilnih kartic** - Kartični podatki so shranjeni pri ponudniku varnostne rešitve, trgovec ne more fizično priti do podatkov.

Ostale zahteve iz tabele 2.2 vsekakor pridejo v poštev. To so zahteve, ki se tičejo vzdrževanja in testiranja varnega omrežja, vzdrževanja programa za upravljanje z ranljivostmi sistema in vzdrževanja varnostne politike. Ker moramo zaščititi dostop do POS terminala, je potrebno implementirati sistem za nadzor nad omrežjem, ki spremlja nedovoljen promet in odtekanje podatkov k neznanim virom. To pomeni omejevanje IP naslovov z znotraj in zunaj omrežja in vpeljavo ostalih varnostnih mehanizmov, ki preprečujejo dostop do POS terminala.

4.5.1 Človeški viri

Zahteve standarda narekujejo vpeljavo varnostne politike v podjetje in letno izobraževanje zaposlenih v zvezi z varnostjo kartičnih podatkov. O varnostni politiki govori Zahteva 12, ki pravi: »Vzdržuj varnostno politiko, ki ureja področje varovanja informacij, ki velja tako za zaposlene kot za zunanje sodelavce«. Zahteva 12 ima 9 podzahtev. Del podzahtev lahko vidimo na sliki poročila o skladnosti 2.3. Podzahteve zahteve 12 narekujejo sledeče. Vzpostaviti je potrebno dnevne postopke osnovnih pregledov varnosti sistema. Organizirati je potrebno izobraževanja zaposlenih o varnostni politiki, preverjanje znanja in seznanjanje z grožnjami. Če občutljive kartične podatke zaupamo tretji osebi, torej ponudniku varnostne rešitve, moramo vsaj enkrat letno na formalen način oceniti, da je njegovo poslovanje in varstvo kartičnih podatkov skladno s standardom PCI DSS. Potrebno je pripraviti tudi načrt v primeru vdora v sistem.

Zaradi velikega števila zaposlenih je potrebno poseči po sodobnih načinih osveščanja. Menim, da je e-izobraževanje dobra izbira, tako cenovno kot tudi s stališča praktičnosti. Moj predlog pri izvedbi projekta je bil, da se izobraževanje zaposlenih izvaja s pomočjo e-učilnice, ki se nahaja na intranetu podjetja.

Na ta način se poenostavi letno poročanje o ohranjanju skladnosti, saj je podatke statistično lahko obdelati, če so v elektronski obliki. Vsak zaposleni ima svojo unikatno identifikacijsko številko in tako lahko učinkovito beležimo, kdo je vprašalnik izpolnil in kdo ne. Za večjo motivacijo zaposlenih, kar se tiče učenja glede varnosti, bi med pravilno izpolnjenimi vprašalniki izžrebali nekoga, ki prejme nagrado (na primer promocijski material). Tovrstni vprašalniki so se v podjetju trgovca v preteklosti že izkazali za učinkovite in mislim, da bi dolgoročno pripomogli k povečanju varnosti v podjetju. Na začetku vprašalnika se bo nahajala izobraževalna literatura, ki jo bo potrebno preučiti, preden se lotimo odgovarjanj na vprašanja. Moja naloga pri projektu vpeljave standarda PCI DSS v podjetje bo napisati učno literaturo na začetku vprašalnika in sestaviti vprašanja za zaposlene. To bom morala redno objavljati na e-učilnici podjetja in poročati o ozaveščenosti zaposlenih z varnostno politiko.

Vsebina vprašalnikov na e-učilnici se bo navezovala na vse kadre, predvsem pa na zaposlene na prodajnih mestih, ki neposredno upravljajo z bančnimi karticami. Zaposleni na prodajnih mestih morajo poznati in izvajati navodila v zvezi z varno uporabo POS terminalov. To pomeni, da morajo vsak dan preveriti POS terminal, da na njem ni bil izvršen neavtoriziran fizični poseg, ki omogoča krajo PIN in PAN številk (ang.: *skimming*). V primeru neavtoriziranega posega v POS terminal, mora prodajno osebje to nemudoma prijaviti klicnemu centru v podjetju trgovca. Zaposleni morajo poznati pravila za varno ravnanje s karticami. Seznanjeni morajo biti z informacijsko varnostno politiko, kjer so napisana pravila o varni uporabi informacijskih sredstev. Pri načinu dviganja ozaveščenosti o varnosti kartičnih podatkov si lahko pomagamo z dokumentom, ki se nahaja na uradni strani Sveta PCI SSC [15].

Poglavje 5

Sklepne ugotovitve

5.1 Ovrednotenje zastavljenih ciljev

Cilj, ki smo si ga zadali, je bil prikaz vpeljave standarda PCI DSS v podjetje velikega trgovca.

V prvem, teoretičnem delu diplomske naloge smo se dobro spoznali s področjem kartične industrije in varnostnim standardom PCI DSS. Dobili smo potrditev, da je vpeljava standarda v podjetje nujna. Z vpeljavo standarda zmanjšamo možnost vdora v podjetje in zlorabe občutljivih podatkov. Izognemo se velikim kaznim, ki so predpisane za podjetja, ki v času vdora niso skladna s PCI DSS. Višina kazni je večja kot je višina stroškov za izvedbo projekta skladnosti s PCI DSS. Poleg izgube ugleda in nezaupanja kupcev v primeru zlorabe njihovih podatkov, nam lahko izdajatelji kartic tudi prepovedo uporabo bančnih kartic. Kar pa lahko pomni celo konec poslovanja in zaprtje podjetja.

V drugem, praktičnem delu smo analizirali možne rešitve za vpeljavo standarda PCI DSS v podjetje. Standard le navaja zahteve, ki jih moramo doseči, ni pa opisano, kako naj te zahteve vpeljemo v podjetje in dosežemo skladnost. Analizirali smo nekaj možnih rešitev, ki so med najpogosteje uporabljenimi. Nekaj od teh je predlagala strokovna literatura, ki jo je izdal Svet PCI SSC. Nekatere izmed rešitev so predlagala specializirana podjetja, ki se kot zunanji ponudniki ukvarjajo z vpeljavo standarda PCI DSS v podjetja, ki jih za to najamejo. Nekatere rešitve so predlagali tudi razni avtorji člankov, ki so izvedenci za standard PCI DSS, na primer kvalificirani ocenjevalci QSA. Analiza je pokazala, da so si rešitve med seboj zelo različne in imajo specifične načine

implementacije. Nekatere rešitve vpeljujejo zunanje ponudnike, ki celotno kartično poslovanje povsem izločijo iz okolja trgovca. Druge rešitve predlagajo korenito spremembo obstoječega sistema trgovca. Rešitev, ki jo želimo, pa mora omogočati prilagodljivost, nizke stroške vpeljave in ohranjanja skladnosti in predvsem zagotoviti varnost podatkov.

Izbrana rešitev temelji na pristopu šifriranja podatkov takoj ob zajemu, s čimer preprečimo, da se po okolju trgovca procesirajo, pošiljajo ali shranjujejo občutljivi kartični podatki v čisti obliki. Ta rešitev je zahtevala nakup novih POS terminalov, razvoj aplikacije, ki teče na POS terminalu, razvoj Osrednje dekripcijske naprave in vpeljavo ponudnika varnostne rešitve.

Izbrana rešitev dosega želene cilje, saj zagotavlja izredno veliko prilagodljivost sistema. Ker smo razširili funkcionalnost POS terminala z lastno aplikacijo, ki teče na terminalu in razvili lastno Osrednjo dekripcijsko napravo, smo postali bolj neodvisni od bank in procesnih centrov in se tako lažje pogajamo za nižje provizije bančnih transakcij. Razvoj svojega POS terminala je bil potreben tudi zaradi množice plačilnih kartic zvestobe ter kartic za poslovne stranke, ki se ne avtorizirajo na banki ali procesnem centru, temveč na osrednjem strežniku trgovca. Če bi najeli banko ponudnico storitve, bi se z njo zavezali, da procesira vse bančne transakcije in zaračuna provizijo. Za vsako kartico, ki ni bančna, bi bile potrebne prilagoditve POS terminala, kar pa povzroča velike stroške. Če bi želeli banko zamenjati, bi morali ponovno menjati celotno POS arhitekturo. Tudi s samostojnim razvojem Osrednje dekripcijske naprave smo pridobili na prilagodljivosti sistema. Osrednjo dekripcijsko napravo lahko zaupamo še kakšnemu drugemu ponudniku varnostne rešitve in tako nismo odvisni več samo od enega.

Ostale rešitve so predlagale korenite spremembe obstoječega sistema, kar pa nebi bistveno zmanjšale PCI obsega. Izbrana rešitev obstoječega sistema nič ne spremeni, edina stvar ki se v okolju trgovca spremeni, tehnično gledano, so POS terminali. Izkazalo pa se je, da smo stare POS terminale tako ali tako želeli zamenjati, saj so bili dotrajani in so povzročali velike stroške vzdrževanja. Našim potrošnikom smo z zamenjavo POS terminalov omogočili brezstično plačevanje s kartico, ki ga stari POS terminali niso podpirali. Tako potrošnikom pri nakupu ni več treba vtakniti kartice v režo na POS terminalu, pri manjših plačilih pa ni potreben vnos PIN kode.

Z vpeljavo ponudnika varnostne rešitve smo močno zmanjšali možnost vdora v sistem in posledično zlorabo kartičnih podatkov. S tem smo dosegli tudi cilj, da dvignemo nivo kartične varnosti. Če občutljivih kartičnih podatkov v

našem okolju ni, potem jih ne more nihče zlorabiti. Z vpeljavo ponudnika ni potrebno toliko virov nameniti vzdrževanju sistema za šifriranje podatkov, ker za to skrbi ponudnik sam.

Ker smo obseg PCI uspeli zmanjšati na minimum, bo tudi dokazovanje skladnosti lažje, hitrejše in cenejše. To pomeni manj dokumentacije in manj testiranja zahtev. Ne bo potrebno zaposlovati novih kadrov zaradi pomoči pri vzdrževanju varnega sistema in pri ohranjanja skladnosti s standardom.

Zahteve standarda narekujejo vpeljavo varnostne politike v podjetje. Tukaj vidimo možnost izboljšave, ki jo je možno doseči na področju varnostne politike in izobraževanja zaposlenih glede varnosti informacij. Dostikrat se namreč zgodi, da imajo ljudje brezbrižen pogled na varnost in se jim to zdi samo strošek. Takega mišljenja se ne da spremeniti v enem dnevu, verjetno tudi ne v enem letu. Poleg objave varnostne politike na navidezni oglasni deski v intranetu podjetja, bi predlagali tudi vprašalnike, ki bi spodbudile ljudi k razmišljanju o varnosti. Vprašalnike bi objavili na e-učilnici podjetja. Med pravilno izpolnjenimi vprašalniki bi izžrebali nekoga, ki prejme nagrado. Tovrstni vprašalniki so se v podjetju trgovca v preteklosti že izkazali za učinkovite. Vprašalniki bi bili relativno kratki, da ne vzamejo preveč časa. To je ponavadi tudi razlog, da jih ljudje ne izpolnijo. Na intranetu pa bi se pojavljali redno, ker kot že omenjeno, težko v enem dnevu spremeniš slabe navade človeka.

Diplomsko delo lahko predstavlja pomoč drugim trgovskim podjetjem, ki se soočajo z vpeljavo standarda PCI DSS, saj vsebuje seznam možnih rešitev za vpeljavo standarda kot tudi prednosti in slabosti le-teh. Glede na velikost podjetja trgovca in način poslovanja, lahko vsak izbere način, ki je najbolj primeren za vpeljavo standarda v njegov sistem.

Ker smo razvili svojo lastno rešitev, vidimo tudi možnost prodaje sistema za šifriranje in dešifriranje podatkov. Komponente tega sistema so aplikacija, ki teče na POS terminalu na enem koncu in Osrednja dekripcijska naprava na drugem. Za nakup rešitve bi se zanimali tako trgovci kot tudi procesni centri oz. ponudniki varnostnih rešitev. Sicer prodaja informacijsko-varnostnih rešitev ni ravno področje našega poslovanja, toda menimo, da bi bilo potrebno podati predlog poslovodstvu in razložiti, da na tak način lahko dobimo nazaj začetno investicijo, namenjeno za ta projekt.

5.2 Zaključek

V diplomskem delu smo opisali standard PCI DSS in zahteve, ki ga sestavljajo. Analizirali smo možne rešitve za vpeljavo standarda v podjetje velikega trgovca. Opisali smo izvedbo izbrane rešitve na konkretnem primeru. Ugotovili smo, da izbrana rešitev dosega želene cilje, ki smo si jih v podjetju zastavili. Potem smo zapisali še predloge za izboljšave.

Menimo, da smo z diplomskim delom dosegli zastavljene cilje, saj smo prikazali izvedbo rešitve, za katero smo ugotovili, da z veliko prilagodljivostjo in relativno nizkimi stroški zagotavlja skladnost podjetja s standardom PCI DSS. Toda dejstvo je, da se na trgu pojavljajo vedno nove tehnologije, nova orodja ter nove rešitve. Danes je izbrana rešitev res optimalna za izbranega trgovca, toda ker se s to tematiko srečujejo vsi trgovci in ostale organizacije, ki sprejemajo bančne kartice, je za pričakovati, da se bo slej ali prej na trgu pojavila boljša, novejša, varnejša rešitev.

Pri vsem tem pa se je potrebno zavedati, da popolne varnosti ni! Obstajajo primeri, ko so bila podjetja skladna s standardom PCI DSS, pa se je vseeno zgodil vdor [19]. Tako kot gre naprej razvoj varnosti, gre naprej tudi razvoj novih načinov napadov na varnostne kontrole, zato nikoli ne smemo zaspati na lovorikah »varnosti«, ki jih dobimo s skladnostjo s katerimkoli varnostnim standardom.

Slike

Tabele

Literatura

[1] Interna dokumentacija podjetja.

[2] E commerce Special Interest Group PCI Security Standards Council. *Information Supplement: PCI DSS E-commerce Guidelines*. PCI Security Standards Council, 2. edition, Januar 2013.

[3] Atos company. YOMANI colourful innovation. Dostopno na: `https://terminals.worldline.com/adminV3/ContentManager/display/000/509/015/5090150.pdf`.

[4] PCI Security Standards Counci. *Payment Card Industry (PCI) Payment Application Data Security Standard*. PCI Security Standards Council, 3. edition, November 2013.

[5] PCI Security Standards Council. About the PCI Security Standards Council. Pogledano 19.12.2014. Dostopno na: `https://www.pcisecuritystandards.org/organization_info/index.php`.

[6] PCI Security Standards Council. Approved PIN Transaction Security (PTS) Devices. Pogledano 3.2.2015. Dostopno na: `https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php`.

[7] PCI Security Standards Council. Approved Scanning Vendors. Pogledano 25.1.2015. Dostopno na: `https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php`.

[8] PCI Security Standards Council. Atos Worldline Yomani. Pogledano 19.12.2014. Dostopno na: `https://www.pcisecuritystandards.org/popups/pts_device.php?appnum=4-30046`.

[9] PCI Security Standards Council. Is encrypted cardholder data in scope for PCI DSS? Pogledano 19.12.2014. Dostopno na: `https://www.pcisecuritystandards.org/faq/`.

[10] PCI Security Standards Council. *Navigating PCI DSS: Understanding the Intent of the Requirements*. PCI Security Standards Council, 1.2 edition, Oktober 2008.

[11] PCI Security Standards Council. *Ten Common Myths of PCI DSS*. PCI Security Standards Council, 2008. Dostopno na: `https://www.pcisecuritystandards.org/pdfs/pciscc_ten_common_myths.pdf`.

[12] PCI Security Standards Council. *Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS): Glossary of Terms, Abbreviations, and Acronyms*. PCI Security Standards Council, 2. edition, Oktober 2010.

[13] PCI Security Standards Council. *PTS Security Requirements Version 3.0 FAQ*. PCI Security Standards Council, 1.2 edition, Maj 2010.

[14] PCI Security Standards Council. *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures*. PCI Security Standards Council, 3. edition, November 2013.

[15] PCI Security Standards Council. *Information Supplement: Best Practices for Implementing a Security Awareness Program*. PCI Security Standards Council, 1. edition, Oktober 2014.

[16] PCI Security Standards Council. *Payment Card Industry (PCI) Data Security Standard Report on Compliance*. PCI Security Standards Council, 1. edition, Februar 2014.

[17] Thomas E. Dickey. ncurses. Pogledano 2.2.2015. Dostopno na: `http://invisible-island.net/ncurses/ncurses.faq.html`.

[18] Paresh Khatri. MPLS - A Tutorial. Pogledano 2.2.2015. Dostopno na: `http://www.sanog.org/resources/sanog14/sanog14-paresh-mpls.pdf`.

[19] Tracy Kitten. Retailer Breaches: A PCI Failure? Pogledano 5.1.2015. Dostopno na: `http://www.bankinfosecurity.com/target-nm-breaches-pci-failure-a-6419/op-1`.

[20] Boulder Rob Braun Panos Tsirigotis. xinetd(8) - Linux man page. Pogledano 2.2.2015. Dostopno na: http://linux.die.net/man/8/xinetd.

[21] Paymetric. 5 Ways Businesses Can Reduce PCI DSS Scope. Pogledano 2.2.2015. Dostopno na: http://www.paymetric.com/blog/5-ways-businesses-can-reduce-pci-dss-scope.

[22] Siva Ram. Derived Unique Key Per Transaction – DUKPT. Pogledano 19.12.2014. Dostopno na: http://www.maravis.com/library/derived-unique-key-per-transaction-dukpt/.

[23] Tokenization Taskforce PCI Security Standards Council Scoping SIG. *PCI DSS Tokenization Guidelines*. PCI Security Standards Council, 2. edition, Avgust 2011.

[24] Wikipedia. Hardware security module. Pogledano 19.12.2014. Dostopno na: http://en.wikipedia.org/wiki/Hardware_security_module.

[25] Wikipedia. Protocol converter. Pogledano 19.12.2014. Dostopno na: http://en.wikipedia.org/wiki/Protocol_converter.

[26] Wikipedia. Triple DES. Pogledano 19.12.2014. Dostopno na: http://en.wikipedia.org/wiki/Triple_DES.